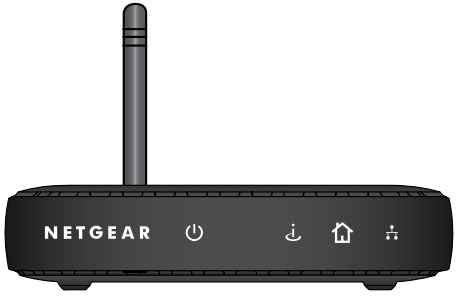
User Manual for the NETGEAR WGE111 Wireless Game Adapter



NETGEAR

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

Version v1.0
July 2004

Technical Support

Please refer to the support information card that shipped with your product. By registering your product at *http://www.netgear.com/register*, we can provide you with faster expert technical support and timely notices of product and software upgrades.

NETGEAR, INC. Support Information

Phone: 1-888-NETGEAR, for US & Canada only. For other countries, see your Support information card.

E-mail: support@netgear.com

Web site: *http://www.netgear.com*

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

July 2004

Certificate of the Manufacturer/Importer

It is hereby certified that the Model WGE111 Wireless Game Adapter has been suppressed in accordance with the conditions set out in the BMPT- AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example,

test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

NETGEAR Wireless Game Adapter WGE111

Tested to Comply
with FCC Standards
FOR HOME OR OFFICE USE

Warning!

To comply with the FCC's exposure requirements you must maintain a distance of at least 1 cm from the antenna of this device while it is in use. This device should not be co-located with other transmitters.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.

2. This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of more of the following measures: (1) Reorient or relocate the receiving antenna, (2) Increase the separation between the equipment and receiver, (3) Connect the equipment into an outlet on a circuit different from that to which the receiver is connected, (4) Consult the dealer or an experienced radio/TV technician for help.

Federal Communications Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (NETGEAR WGE111 Wireless Game Adapter) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

FCC ID: PY3WGE111-F

Canada ID: 4054A-WGE111F

CE0336!

Japan ID: 003NY03050

VCCI Statement

This equipment is in the Class B category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas. When used near a radio or TV receiver, it may become the cause of radio interference. Read instructions for correct handling.

Contents

Chapter 1
About This Manual

Thank you for purchasing the NETGEAR WGE111 Wireless Game Adapter.

Audience, Conventions, Scope

This reference manual assumes that the reader has basic-to-intermediate computer and Internet skills. However, basic computer network, Internet, and firewall technologies tutorial information is provided in the Appendices, on the *NETGEAR WGE111 Wireless Game Adapter Resource CD*, and on the NETGEAR Web site.

This guide uses the following typographical conventions:

Table 1. Typographical conventions

italics	Emphasis, books, CDs, URL names
bold times roman	User input
`courier font`	Screen text, file and server names, extensions, commands, IP addresses

Note: This format is used to highlight information of importance or special interest.

This manual is written for the WGE111 Wireless Game Adapter according to these specifications:

Table 1-1. Manual Specifications

Product Version	NETGEAR WGE111 Wireless Game Adapter
Manual Publication Date	August 2004

Note: Product updates are available on the NETGEAR, Inc. Web site at *http://www.netgear.com/support/main.asp*.

How to Use this Manual

The HTML version of this manual includes these features.

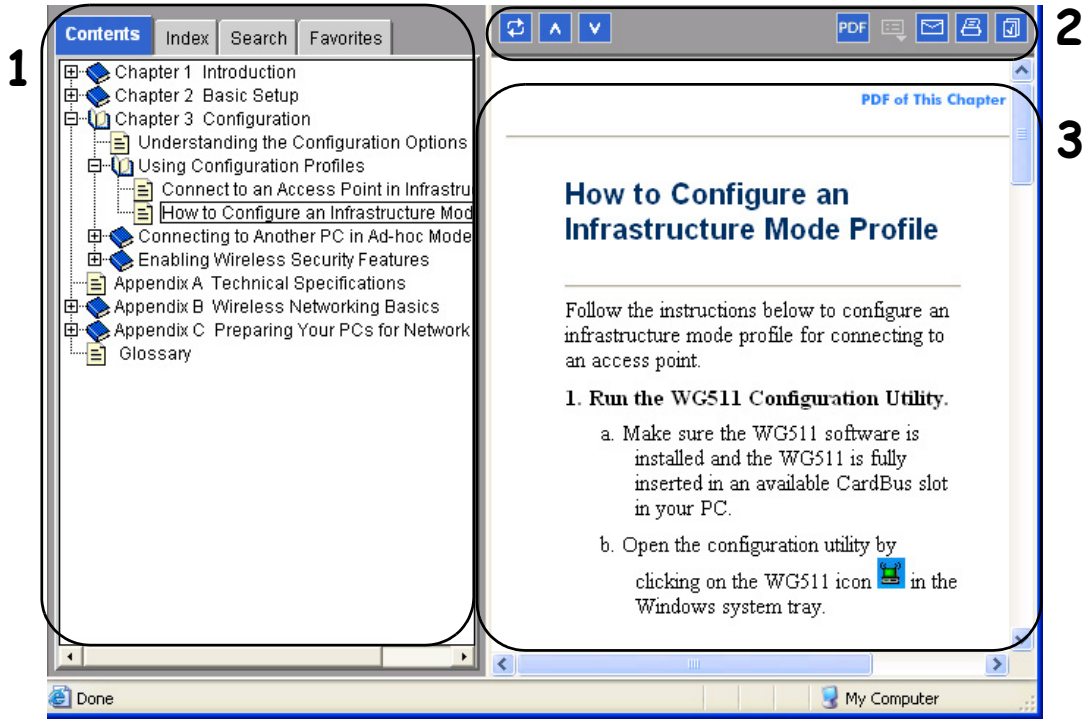


Figure 1 -1: HTML version of this manual

1. **Left pane**. Use the left pane to view the Contents, Index, Search, and Favorites tabs.

   To view the HTML version of the manual, you must have a version 5 or later browser with JavaScript enabled.

2. **Toolbar buttons**. Use the toolbar buttons across the top to navigate, print pages, and more.

   – The *Show in Contents* button locates the current topic in the Contents tab.

   – *Previous/Next* buttons display the previous or next topic.

   – The *PDF* button links to a PDF version of the full manual.

–  The *Print* button prints the current topic. Using this button when a step-by-step procedure is displayed will send the entire procedure to your printer—you do not have to worry about specifying the correct range of pages.

3. **Right pane**. Use the right pane to view the contents of the manual. Also, each page of the manual includes a PDF of This Chapter link at the top right which links to a PDF file containing just the currently selected chapter of the manual.

How to Print this Manual

To print this manual you can choose one of the following several options, according to your needs.

- **Printing a "How To" Sequence of Steps in the HTML View**. Use the Print button on the upper right side of the toolbar to print the currently displayed topic. Using this button when a step-by-step procedure is displayed will send the entire procedure to your printer—you do not have to worry about specifying the correct range of pages.
- **Printing a Chapter**. Use the PDF of This Chapter link at the top right of any page.
  - Click the "PDF of This Chapter" link at the top right of any page in the chapter you want to print. A new browser window opens showing the PDF version of the chapter you were viewing.
  - Click the print icon in the upper left of the window.
  - **Tip**: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.
- **Printing the Full Manual**. Use the PDF button in the toolbar at the top right of the browser window.
  - Click the PDF button. A new browser window opens showing the PDF version of the chapter you were viewing.
  - Click the print icon in the upper left side of the window.
  - **Tip**: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

Chapter 2
Introduction

This chapter introduces the features, package contents, and appearance of the NETGEAR WGE111 Wireless Game Adapter.

About the NETGEAR WGE111 Wireless Game Adapter

Congratulations on your purchase of the NETGEAR® WGE111 Wireless Game Adapter. NETGEAR wireless game adapters are fast and easy to set up with NETGEAR wireless game adapter configuration software. With Microsoft Internet Explorer or Netscape Web browser, you can configure the wireless game adapter even easier. This manual describes the installation and use of the WGE111 for operation with a Microsoft® Windows® XP, Windows® 2000, Windows® Me, Windows® 98SE 2nd edition, or Windows NT 4.0 (with Service Pack 5 or above) system.

For quick installation and setup, please see the NETGEAR WGE111 Wireless Game Adapter Installation Guide. This manual describes in detail how to set up the Model WGE111 wireless game adapter and provides you with further reference information.

Chapter 3, “Basic Setup” provides information on the NETGEAR Wireless Game Adapter Smart Wizard Configuration Assistant, a program developed by NETGEAR for fast and easy device configuration. There is also a built-in Web server in the wireless game adapter so you can use a Web browser to configure the WGE111 Wireless Game Adapter, as described in Chapter 4, “Web Configuration”.

Key Features and Related NETGEAR Products

The key features of the WGE111 Wireless Game Adapter are:

- Extremely compact size.
- Easy configuration of the device with NETGEAR Wireless Game Adapter software that assures fast and easy setup for Windows 98, Windows Me, Window NT, Windows 2000, and Windows XP.
- Web browser interface provides an easy way to configure the WGE111 Wireless Game Adapter in a TCP/IP network.
- RJ-45 Ethernet port to connect to a game console or a computer. The port is 10/100 BASE-T standard Ethernet capable. It can be used to connect to a 10/100 Mbps hub or switch for configuration of the wireless game adapter.
- MAC Address cloning support. The WGE111 Wireless Game Adapter automatically clones the Media Access Control (MAC) address of the device connected on its LAN port.

What's in the Box?

The product package should contain the following items:

- WGE111 Wireless Game Adapter
- AC Power adapter — 5V, 2A
- Ethernet cable
- Installation Guide for the NETGEAR WGE111 Wireless Game Adapter
- *NETGEAR WGE111 Wireless Game Adapter Resource CD*, including:
  - — User Manual for the NETGEAR WGE111 Wireless Game Adapter
  - — Animated Network Properties Configuration Tutorial
  - — PC Networking Tutorial
- Warranty & Registration card
- Support information card

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the product for repair.

To qualify for product updates and product warranty registrations, fill out the registration information within 30 days of purchase. For priority service, register online on the NETGEAR Web page at:

http://www.NETGEAR.com/support/main.asp

You can also fill out and return the Warranty & Registration Card that is included in your product package.

Hardware Description

The Model WGE111 Wireless Game Adapter LEDs indicate the status of the server and the Ethernet traffic. It has one 10/100 Mbps network port. The port operates in 10/100 Mbps when connected to a 10/100Mbps Ethernet network. It has a power adapter receptacle that accepts a 5V, 2A DC power adapter. It has a reset button.

As illustrated in the figure below, the WGE111 Wireless Game Adapter has 4 LEDs.

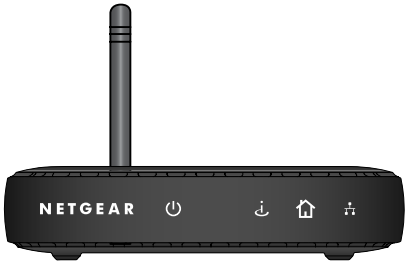


Figure 2-1: Front of the WGE111 Wireless Game Adapter

Status Indicators and Ports of the WGE111

See the table below for a description of the LED indicator lights:

Table 2-1. LED Descriptions

Label	Activity	Description
 Power	On Off	Power is supplied to the wireless game adapter. Power is not supplied to the wireless game adapter.
 Internet	On (Green) Fast Blink Slow Blink	The Internet (Wide Area Network) port has detected a link with an attached device. Data is being transmitted or received by the Internet port. Searching for wireless network.
 Ad-Hoc	On (Blue) Fast Blink Slow Blink	The Ad-Hoc port has detected a link with an attached device. Data is being transmitted or received by the Ad-Hoc port. Searching for ad-hoc connection.
 Ethernet	On (Green) Blink Off	The Ethernet local (LAN) port has detected link with a 10 or 100 Mbps device. Data is being transmitted or received. No link is detected on this port.

Reset Push Button

The button is recessed; a pin or paper clip can be used to press it. This button is used to restore the wireless game adapter to the default settings.

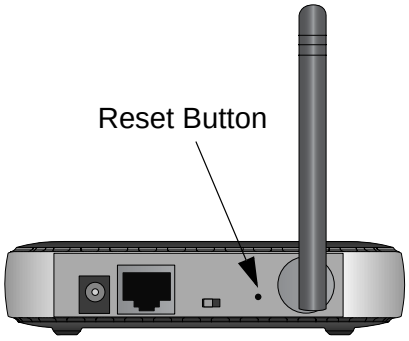


Figure 2-2: Back of the WGE111 Wireless Game Adapter

To restore the factory default settings:

1. Press and hold the reset button (located beside the antenna in the diagram above).
2. The LEDs start to flash. Release the reset button after 5 seconds and the LEDs will flash faster, then the system will reboot and reset to the factory defaults.

Chapter 3
Basic Setup

This chapter describes how to install your NETGEAR WGE111 Wireless Game Adapter and set up basic connectivity on your Local Area Network (LAN).

Preparing to Install Your WGE111 Wireless Game Adapter

The NETGEAR WGE111 Wireless Game Adapter is plug-and-go so that you can set it up immediately without configuration. The following scenarios are presented in this chapter:

- "Game Console Plug-and-Go Scenario" on page 3-4
- "Personal Computer Plug-and-Go Scenario" on page 3-5

If you need to change the default IP address or set wireless security, you can use the Smart Wizard configuration assistant to identify your network configuration settings. After you have used the Smart Wizard, you can access the WGE111 Wireless Game Adapter configuration from a Web browser using the TCP/IP address of the WGE111.

1. First, determine your network configuration. See "Planning the WGE111 Wireless Game Adapter Configuration" on page 3-6.
2. Second, use the Smart Wizard configuration assistant to configure your initial settings. See "Using the NETGEAR Smart Wizard Configuration Assistant" on page 3-9.
3. If you would like to use the Web configuration interface, see Chapter 4, "Web Configuration".

System Requirements

Before installing the WGE111 Wireless Game Adapter, please make sure that these minimum requirements have been met:

- For connecting into a wired network, you must have the network set up and working with an access point or wireless router.
- For creating an Ad-Hoc network without an access point, all devices must have a receiver/transmitter. (The receiver/transmitter may be another WGE111 Wireless Game Adapter adapter.)

If the default settings do not work, you will need to configure the WGE111 Wireless Game Adapter. Also, if you have more than one WGE111 in the network, only one can use the default IP address. You'll have to configure the others with unique IP addresses. To configure the WGE111 Wireless Game Adapter, you must have a personal computer with Internet browser software installed, such as Microsoft® Internet Explorer 5.0 (or later) or Netscape® 6.0 (or later).

Placement and Range Guidelines

Computers and other Ethernet-enabled devices can connect over wireless networks indoors at more than 500 feet. However, the operating distance or range of your wireless connection can vary significantly based on the physical location of the WGE111 Wireless Game Adapter. For best results, avoid potential sources of interference, such as:

- Large metal surfaces
- Microwaves
- 2.4 GHz cordless phones

In general, wireless devices can communicate through walls. However, if the walls are constructed with concrete or have metal (or metal mesh), the effective range will decrease if such materials are between the wireless devices.

Operating Modes

The WGE111 Wireless Game Adapter operates in either Infrastructure or Ad-Hoc mode.

Mode	Switch Position	Your System
Infrastructure mode (labeled Internet)	Left position, which is the factory shipped default	Access point or wireless router connected to a wired network
Ad-Hoc mode	Right position (must be changed from default left position)	Small, wireless-only network and all devices have wireless transmitters/ receivers.

Note: If you are using Ad-Hoc mode and have more than one NETGEAR WGE111 Wireless Game Adapter, you need to use the Smart Wizard configuration assistant to change the IP settings and ensure unique IP addresses. Each WGE111 Wireless Game Adapter is set by default to use the IP address 192.168.0.202. See "Using the NETGEAR Smart Wizard Configuration Assistant" on page 3-9 for information on changing the IP addresses of the wireless game adapter.

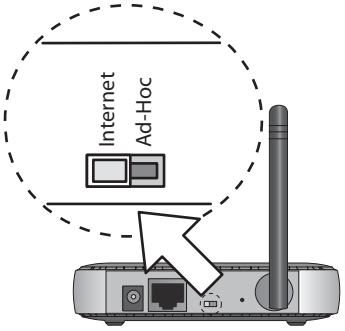


Figure 3-1: Switch on back of wireless game adapter sets Infrastructure or Ad-Hoc mode

The switch is set to the left for Infrastructure mode (labeled Internet) or to the right for Ad-Hoc mode.

Note: The WGE111 Wireless Game Adapter is factory-shipped with the switch on the rear panel set to the left, which indicates Infrastructure mode. The wireless game adapter can be plugged into a game console or computer directly without configuration.

Game Console Plug-and-Go Scenario

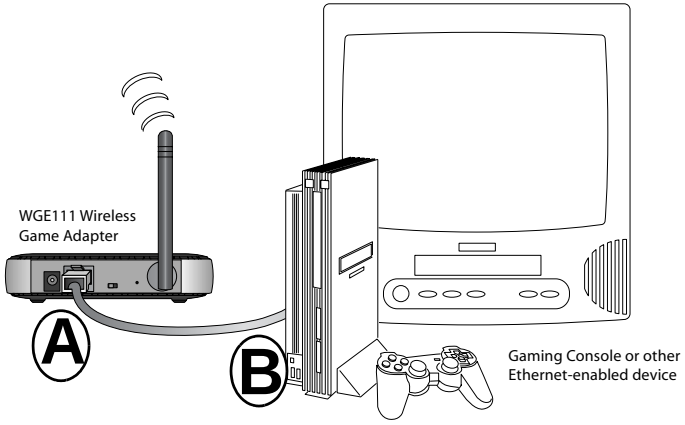


Figure 3-2: Internet Game Console Scenario

What you need.

- Broadband Internet access through a router with an 802.11b or 802.11g wireless access point (built in to the router or separate) without any security features enabled.

  Note: If you enabled security features (like WEP, SSID broadcast off, MAC filtering, etc.) you need to follow the instructions given in "Using the NETGEAR Smart Wizard Configuration Assistant" on page 3-9.

- A network-enabled game console.

What you do.

1. Connect the Ethernet cable from your WGE111 Wireless Game Adapter (**A**) to the Ethernet port (**B**) in the game console.
2. Make sure that the switch on the back of the WGE111 is set to the left side (labeled Internet), which corresponds to Infrastructure Mode.
3. Connect the power adapter to the WGE111 and verify the following:
   -  The power light goes on.
   -  The Internet light is lit.
   -  The Ethernet light is lit when connected to a network-enabled game console.
4. Enjoy your Internet gaming!

Note: Follow the instructions in your PS2 or Xbox manual to configure the IP, DNS, and other parameters of your game console. If you want to change the default IP address or configure the WGE111 Wireless Game Adapter from a Web browser, see "Planning the WGE111 Wireless Game Adapter Configuration" on page 3-6 and "Using the NETGEAR Smart Wizard Configuration Assistant" on page 3-9.

Personal Computer Plug-and-Go Scenario

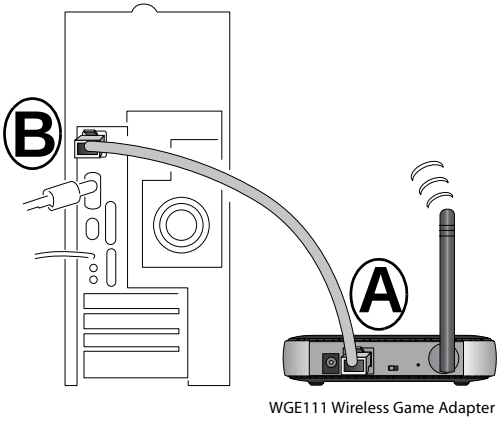


Figure 3-3: Personal Computer Scenario

What you need.

- Broadband Internet access through a router with an 802.11b or 802.11g wireless access point (built in to the router or separate) without any security features enabled.
- A computer to run the initial configuration.

What you do.

1. Connect the Ethernet cable from your WGE111 Wireless Game Adapter (**A**) to the Ethernet port on your computer (**B**).
2. Make sure that the switch on the back of the WGE111 is set to the left side (labeled Internet), which corresponds to Infrastructure Mode.
3. Connect the power adapter to the WGE111 and verify the following:
   - The power light goes on.
   - The Internet light is lit.
   - The Ethernet light is lit.

4. Enjoy your Internet gaming!

Note: If you want to change the default IP address or configure the WGE111 Wireless Game Adapter from a Web browser, see "Planning the WGE111 Wireless Game Adapter Configuration" on page 3-6 and "Using the NETGEAR Smart Wizard Configuration Assistant" on page 3-9.

Planning the WGE111 Wireless Game Adapter Configuration

The WGE111 Wireless Game Adapter is plug-and-go so you do not need to configure it unless you want to change the wireless security settings to match your network, or change the default IP address of 192.168.0.202.

- Windows management — the Smart Wizard configuration assistant installs the NETGEAR WGE111 Wireless Game Adapter software on your computer. You can change your IP configuration using the Smart Wizard as described in the next section, "Using the NETGEAR Smart Wizard Configuration Assistant" on page 3-9.
- Web management — use a Web browser, like Microsoft Internet Explorer or Netscape, to configure your NETGEAR Wireless Game Adapter. Web browser configuration is described in Chapter 4, "Web Configuration".

Note: Troubleshooting information on basic functioning, TCP/IP settings, Web configuration interface, restoring the default configuration and password is described in Chapter 5, "Troubleshooting".

Planning for TCP/IP Configuration

If you are planning to use TCP/IP configuration of the Wireless Game Adapter, you need to determine whether to use a DHCP server-assigned address or a static IP address. This section describes the advantages of these options.

Dynamic IP using DHCP

You can select Obtain IP Address automatically for a dynamic IP address. If you have a home gateway/router, it comes with a DHCP server. When you select this option, the gateway/router assigns the IP address.

Fixed IP

NETGEAR recommends you set up a fixed IP address for the WGE111 Wireless Game Adapter so you can use a Web browser for configuration.

If you are using a NETGEAR router with the default settings, the following settings should work for the Wireless Game Adapter:

- **IP address:** 192.168.0.202 (The first three sections of numbers — 192.168.0 in this example — should match the first three sections of the IP address of your router. Make sure the last three digits in the fourth section are unique on your network.)
- **Subnet mask:** 255.255.255.0
- **Gateway IP address:** 192.168.0.1 or 192.168.1.1 (the address of your router)

Understanding WEP Authentication and Encryption

Restricting wireless access to your network prevents intruders from connecting to your network. However, the wireless data transmissions are still vulnerable to snooping. Using the WEP data encryption settings described below will prevent a determined intruder from eavesdropping on your wireless data communications. Also, if you are using the Internet for such activities as purchases or banking, those Internet sites use another level of highly secure encryption called SSL. You can tell if a Web site is using SSL because the Web address begins with HTTPS rather than HTTP.

Authentication Scheme Selection

The WGE111 lets you select the following wireless authentication schemes.

- **Automatic** — the router detects the authentication scheme.
- **Open System** — allows any device to join the network, assuming that the device SSID matches the access point SSID. Alternatively, the device can use the “ANY” SSID option to associate with any available Access Point within range, regardless of its SSID.
- **Shared Key** — only those computers that possess the correct authentication key can join the network.

Note: The authentication scheme is separate from the data encryption. You can choose an authentication scheme which requires a shared key, but still leave the data transmissions unencrypted. If you require strong security, use both the Shared Key authentication scheme and WEP encryption settings.

Be sure to set your wireless adapter according to the authentication scheme used on your router or access point. Please refer to “Authentication and WEP” on page C-2 for a full explanation of each of these options, as defined by the IEEE 802.11 wireless communication standard.

Encryption Strength Choices

Please refer to "Overview of WEP Parameters" on page C-5 for a full explanation of each of these options, as defined by the IEEE 802.11 wireless communication standard.

- **Disable.** No encryption will be applied. This setting is useful for troubleshooting your wireless connection, but leaves your wireless data fully exposed.
- **64-bit or 128-bit WEP.** When 64-bit or 128-bit is selected, WEP encryption will be applied.

If WEP is enabled, you can manually or automatically program the four data encryption keys. These values must be identical on all computers and access points in your network.

There are two methods for creating WEP encryption keys:

- **Passphrase**. Enter a word or group of printable characters in the Passphrase box and click the Generate button. These characters *are* case sensitive.
- **Manual**. For 64-bit WEP, enter 10 hexadecimal digits (any combination of 0-9, a-f, or A-F). For 128-bit WEP, enter 26 hexadecimal digits (any combination of 0-9, a-f, or A-F). These values *are not* case sensitive.

Understanding WPA-PSK Encryption Security

Wi-Fi Protected Access (WPA) is wireless security with far greater protection than WEP. WPS-PSK (pre-shared key) uses encryption of a shared key as the starting point. WPA has a significant advantages over WEP — an encryption key differing in every packet. It is extremely difficult for hackers to read messages even if they have intercepted the data.

The Passphrase must be 8 to 64 characters in length. The 256 bit key used for encryption is generated from this passphrase. Please refer to "WPA Wireless Security" on page C-8 for more information on WPA-PSK security.

Using the NETGEAR Smart Wizard Configuration Assistant

The Smart Wizard configuration assistant works for WGE111 Wireless Game Adapters used in a Microsoft Windows networking environment. To install and set up your network and the NETGEAR Wireless Game Adapter, you can use a PC with a Microsoft Windows (95, 98, NT 4.0, ME, 2000, or XP) operating system and with the TCP/IP protocol enabled.

You can use the NETGEAR Smart Wizard configuration assistant to change the IP settings of the router. Configuring the WGE111 Wireless Game Adapter to use a fixed or dynamic IP address will allow you to access the wireless game adapter configuration from a Web browser.

1

Connect the Ethernet cable to the WGE111 Wireless Game Adapter and the PC

Note: You must connect an Ethernet cable from the WGE111 to a PC to perform the initial configuration.

a. Connect one end of the Ethernet cable to the Wireless Game Adapter.

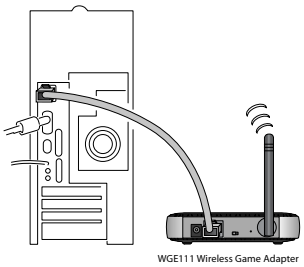
b. Connect the other end of the cable to the Ethernet port on the PC.

c. Connect the power adapter's cord into the back of the Wireless Game Adapter.

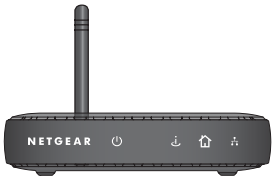
d. Plug the adapter into a power source (such as a wall socket or power switch).

When power has been applied to the WGE111 Wireless Game Adapter, the following LED lights on the front panel should be green:

Power Ethernet



Personal Computer



Check the Power and Ethernet lights on the front of the WGE111 Wireless Game Adapter

2

Start the WGE111 Wireless Game Adapter Smart Wizard Configuration Assistant.

a. Start the NETGEAR Wireless Game Adapter Smart Wizard configuration assistant by inserting the *Resource CD* in your CD-ROM drive.

   Double-click `setup.exe` if the program does not start automatically.

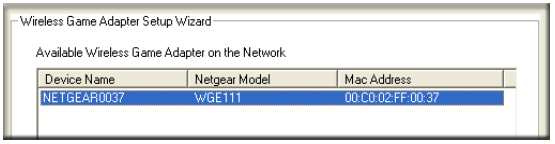
Wireless Game Adapter Setup Screen

b. Select Configuration Assistant.

c. The Wireless Game Adapter Setup Wizard window shows all the NETGEAR Wireless Game Adapters on the LAN.

   Click the Refresh button to see any new Wireless Game Adapters added while the program is running. If you still do not see the Wireless Game Adapter you want to configure, wait a minute and click the Refresh button again.

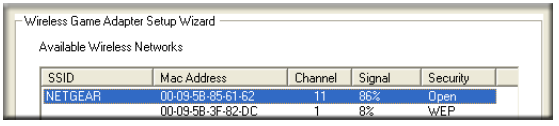
   Click Next.



Select the WGE111 Wireless Game Adapter

d. If the password prompt is displayed, type **password**.

e. Select the Wireless Network to connect to. Click Next.



Select the wireless network

3

Select the Infrastructure and/or Ad-Hoc mode network settings.

Note: You can fill in both sections and the configuration used will be determined by the physical placement of the switch on the back of the wireless game adapter.

a. Fill in the Infrastructure settings. The default SSID is ANY.

b. Select your country/region from the drop-down list.

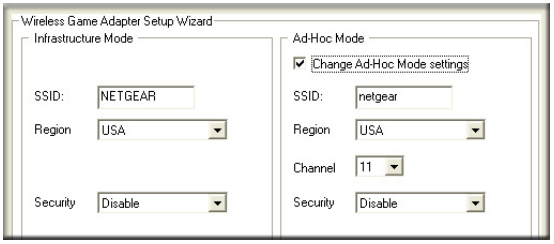
c. Security is disabled by default. Security options are:

- Disable — used for first time configuration.
- WEP — select the Authentication type. Type a Passphrase and click Generate to have the keys generated, or type the keys manually.
- WPA-PSK — type a Passphrase.

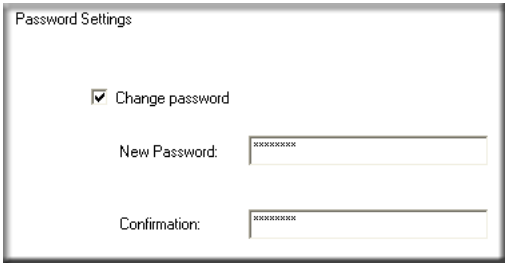
d. If you want to configure Ad-Hoc mode also, select the Ad-hoc Mode check box and configure the Ad-Hoc settings.

e. Click Next.

f. Select the Change Password check box and type the old password for the WGE111 Wireless Game Adapter. The default password is **password**. Type a new password and then type it again in the Confirmation box. Click Next.



Select the Infrastructure or Ad-Hoc settings



Change the Password

4

Select the TCP/IP Settings.

If you are using TCP/IP, select the TCP/IP settings. If you are using more than one WGE111 Wireless Game Adapter on your network, you should change the IP address on one wireless game adapter to prevent conflicts.

a. The next Wireless Game Adapter Setup Wizard window shows the LAN settings for the wireless game adapter. You can change the device name of the wireless game adapter or leave it set to the default.

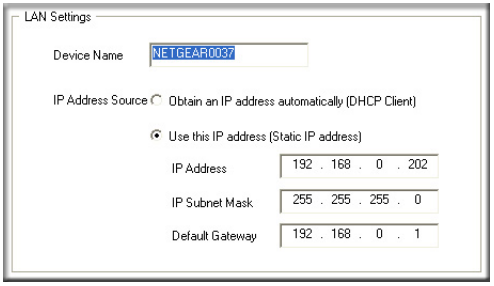
b. NETGEAR recommends using a static IP address so you can use a Web browser to configure the Wireless Game Adapter.

c. If you are going to use a static IP address, select Use this IP Address. Enter the IP Address, IP Subnet Mask, and Default Gateway to match your network.

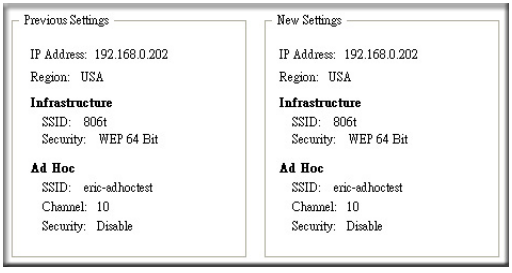
d. Make your selections and click Next.

e. The previous settings (if any) and new settings you have configured are displayed. Your new values will be saved only if you click Next on this screen.

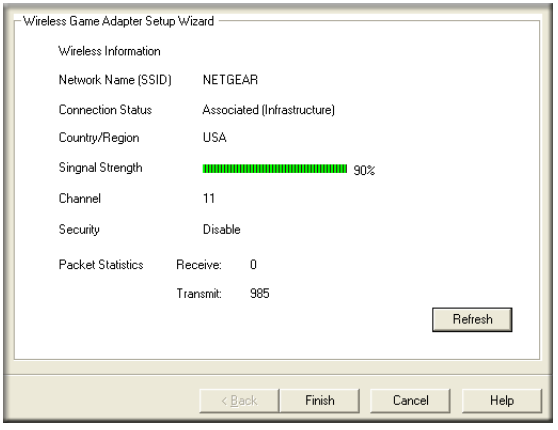
f. The settings you selected are displayed. Click Refresh to update the results. Click Finish to exit.



Select the TCP/IP Settings



Confirm your new settings



WGE111 Wireless Game Adapter settings

Chapter 4
Web Configuration

This chapter contains information about configuring your NETGEAR WGE111 Wireless Game Adapter using the Wireless Game Adapter's browser interface. The Web browser interface provides an easy way to configure the Wireless Game Adapter in a TCP/IP network. You can configure your NETGEAR WGE111 Wireless Game Adapter using any Web browser such as Microsoft Internet Explorer or Netscape Navigator. NETGEAR recommends you use browser versions 5.0 and above.

Once you are logged into the configuration software, you can view the status of your wireless network and the wireless game adapter's current configuration, change the password, enable WEP or WPA-PSK security (if you have it set up on your wireless network), select a specific network for the wireless connection, or make other configuration changes.

Configuring the Wireless Game Adapter Using TCP/IP

Using a Web browser to configure a NETGEAR Wireless Game Adapter requires both the Wireless Game Adapter and the workstation on to be configured for TCP/IP. This is the default for most computers sold in the last few years.

NETGEAR WGE111 Wireless Game Adapters can obtain an IP address automatically using DHCP. If you have a DHCP server (most broadband routers have this feature), the WGE111 will get its own IP address settings for TCP/IP. However, NETGEAR recommends using a static IP address so you can configure the Wireless Game Adapter with a Web browser using the same address each time.

You can also reset the IP address of the Wireless Game Adapter using the NETGEAR Smart Wizard configuration assistant. See “Using the NETGEAR Smart Wizard Configuration Assistant” on page 3-9 for more information.

Connecting to the Wireless Game Adapter

In order to configure the Wireless Game Adapter through a browser interface, your computer must have a Web browser program installed such as Microsoft Internet Explorer or Netscape Navigator.

Note: The IP address of the WGE111 Wireless Game Adapter must be on the same subnet as your access point/router.

1. Start your Web browser.
2. In the Address box, type http:// followed by the IP Address of the Wireless Game Adapter. For example, enter the default IP Address of **http://192.168.0.202** and click Enter.
3. You will then be prompted for the user name and password. Enter password for the password, or whatever password you set using the NETGEAR Smart Wizard configuration assistant.
4. Use the menu selections listed on the left of the screen to move about.

Note: Remember to save modifications made on any screen by clicking the Save button before changing to a different screen.

Viewing the Wireless Game Adapter Status

The Status screen displays current settings and statistics for your WGE111 Wireless Game Adapter. As this information is read-only, any changes must be made on other pages. Click the Refresh button to refresh information on this screen. The figure below shows the Status screen.

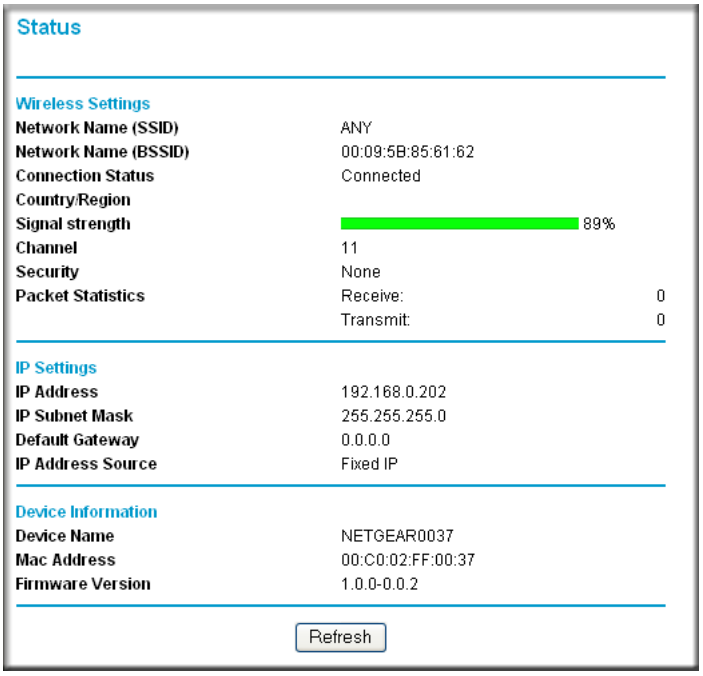


Figure 4-1: Status screen

Wireless Settings

- Network Name (SSID) — the current Wireless Network Name (SSID) value. The default for Infrastructure mode is ANY and the default for Ad-Hoc mode is netgear.
- Network Name (BSSID) — the Basic Service Set Identifier (BSSID) value, which is a 48 bit identity.
- Connection Status — the current connection status of the wireless game adapter.
- Country/Region — the current country setting.
- Signal Strength — the current signal strength.
- Channel — the channel currently in use.
- Security — the current security settings.
- Packet Statistics — the traffic statistics for the wireless interface.

IP Settings

- IP Address — the current IP address.
- IP Subnet Mask — the network mask associated with the IP address.
- Default Gateway — the Gateway IP address associated with the IP address.
- IP Address Source — indicates the current IP Address Source.

Device Information

- Device Name — the current WGE111 Wireless Game Adapter name.
- Mac Address — the current Mac Address.
- Firmware Version — the current Firmware version.

Configuring the Adapter for Infrastructure Mode Access

The Infrastructure Wireless Settings screen is used to change the WGE111 Wireless Game Adapter name and to enable or disable the network security. Select Infrastructure Wireless Settings to configure Infrastructure access, as shown in the screen below.

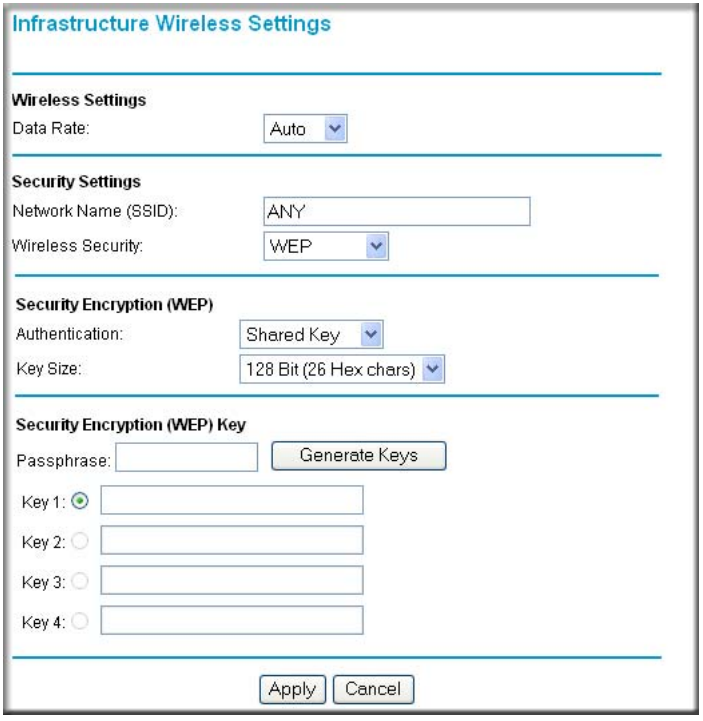


Figure 4-2: Infrastructure mode configuration screen

Data Rate

Select the desired data rate. The options are:

- Auto — the data rate will be detected automatically.
- g only — operates in 802.11g mode only.
- b only — operates in 802.11b mode only.

The data rate is set to Auto by default.

Network Name (SSID)

Choose a descriptive name for the WGE111 Wireless Game Adapter for identification purposes. ANY is the factory default name for Infrastructure mode, which is a special name that will connect with whatever access point or router's signal is strongest. Enter a value of up to 32 alphanumeric characters, or click the Select AP to choose an available Access Point. Spaces are not allowed, but dashes (-) and underscore marks (_) are accepted.

The SSID must be the same as the Access Point you want to connect to. This value is also case-sensitive. For example, NETGEAR is not the same as NETGEAr.

Wireless Security

Select the option to match the Access Point; the screen will change according to the option selected:

- Disable — no data encryption.
- WEP (Wired Equivalent Privacy) — use WEP 64 or 128 bit data encryption. See the next section, "Using WEP Security Encryption" on page 4-6 for detailed information.
- WPA-PSK (Wi-Fi Protected Access Pre-Shared Key) — use WPA-PSK standard encryption. See "Using WPA-PSK Security Encryption" on page 4-7 for detailed information.

Using WEP Security Encryption

Authentication Type

Select Open System or Shared Key authentication, as used by the Access Point. You can select Auto to have the wireless game adapter automatically determine the type.

Key Size

Select the WEP Encryption level to match the Access Point:

- 64-bit (sometimes called 40-bit) encryption
- 128-bit (sometimes called 104-bit) encryption

If using WEP, you can manually or automatically program the four data encryption keys. These values must be identical on all PCs and Access Points in your network.

Automatic Key Generation (Passphrase)

Enter a word or group of printable characters in the Passphrase box and click the Generate button to automatically configure the WEP Key(s). If encryption strength is set to 64 bit, then each of the four key boxes will automatically be populated with key values. If encryption strength is set to 128 bit, then only the selected WEP key box will automatically be populated with key values.

Manual Entry Mode

Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key box.

- For 64 bit WEP — enter ten hexadecimal digits (any combination of 0-9, A-F).
- For 128 bit WEP — enter twenty-six hexadecimal digits (any combination of 0-9, A-F).

Be sure to click Apply to save your settings.

Using WPA-PSK Security Encryption

Enter a word or group of printable characters in the Passphrase box. The Passphrase must be 8 to 64 characters in length. The 256 Bit key used for encryption is generated from this passphrase.

Configuring the Wireless Game Adapter for Ad-Hoc Mode

You can use the WGE111 Wireless Game Adapter in a wireless-only network where the wireless devices are all set to Ad-Hoc mode. By default, the wireless game adapter is set to Infrastructure mode; therefore, you will need to set the switch on the back of the wireless game adapter to the right, which corresponds to Ad-Hoc mode.

In an Ad-Hoc network, all devices must have the same SSID, WEP settings, and IP network subset address with a unique identifying number (xxx.xxx.xxx.yyy).

Select Ad-Hoc Wireless Settings to configure Ad-Hoc access, as shown in the screen below.

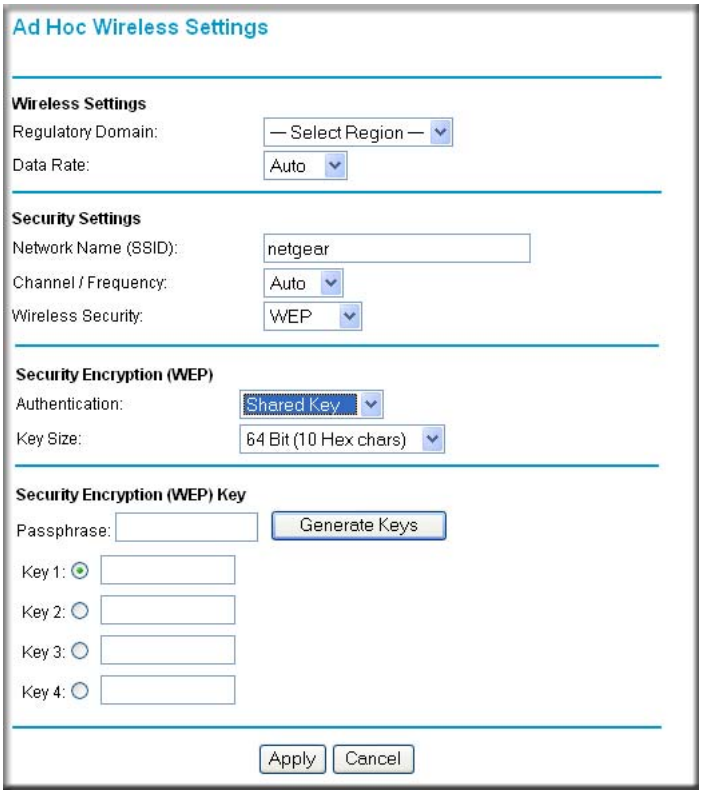


Figure 4-3: Ad-Hoc mode configuration screen

To configure the WGE111 for Ad-Hoc access:

1. Set the Regulatory Domain, which is the country/domain. Select your region from the drop-down list. This field displays the region of operation for which the wireless interface is intended. It may not be legal to operate the router in a region other than the region shown here. If your country or region is not listed, please check with your local government agency or check our web site for more information on which channels to use.

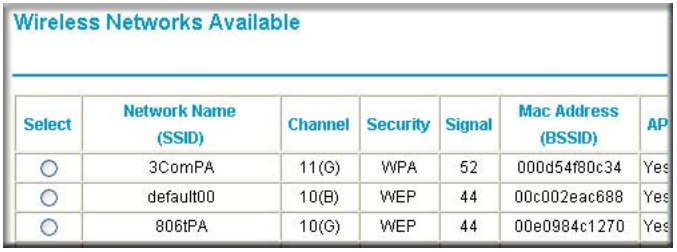
Note: To ensure proper agency compliance and compatibility between similar products in your area; the operating Channel/Frequency & Regulatory Domain must be set correctly.

2. Select the Data Rate — g only, b only, or Auto to have the wireless game adapter automatically determine the data rate to use.
3. Type a Service Set Identifier (SSID) for the network in the SSID box.

4. The default Channel/Frequency is set to Auto. It should not be necessary to set the wireless channel unless you notice interference problems with another nearby access point.
5. Select the Wireless Security option to match the Access Point; the screen will change according to the option selected.
   - Disable — no data encryption.
   - WEP (Wired Equivalent Privacy) — use WEP 64 or 128 bit data encryption. See "Using WEP Security Encryption" on page 4-6 for more information.
6. Click Apply.

Viewing the Wireless Networks Available

This Wireless Networks Available screen shows the wireless networks that the WGE111 Wireless Game Adapter detects.


Wireless Networks Available

Select	Network Name (SSID)	Channel	Security	Signal	Mac Address (BSSID)	AP
○	3ComPA	11(G)	WPA	52	000d54f80c34	Yes
○	default00	10(B)	WEP	44	00c002eac688	Yes
○	806tPA	10(G)	WEP	44	00e0984c1270	Yes

Figure 4-4: Wireless Networks Available

The Network Name (SSID), Channel, Security, Signal Strength, MAC (Media Access Control) address and Access Point network mode for each network are displayed.

Click Scan to search for the wireless networks available. Click Refresh to update the results.

Configuring the IP Settings

The TCP/IP configuration screen is used to configure the IP address of the Wireless Game Adapter. The figure below shows the TCP/IP configuration screen.

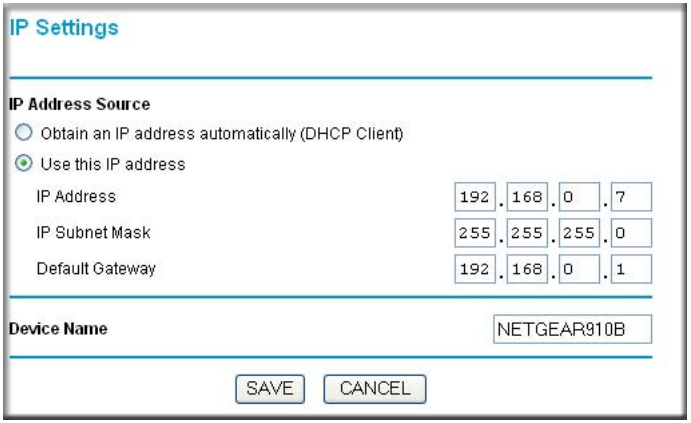


Figure 4-5: IP Settings configuration screen

The default values are suitable for most users and situations.

For the IP Address Source, select Obtain an IP address automatically (DHCP Client) if you have a DHCP Server on your LAN. Otherwise, select Use this IP address and enter the following IP settings:

- IP Address — the IP address is assigned to the Wireless Game Adapter. If you have a private LAN and do not plan to connect to the TCP/IP based internet, NETGEAR recommends that you use an address from the IETF-designated private address list (for example, 192.168.x.x or 10.x.x.x). The first three numbers should match the numbers in the Gateway address and the last number needs to be unique on the network.
- Subnet Mask — the subnet mask defines the range of addresses that are reachable on your local LAN. For example, in a network with a NETGEAR router, the default subnet mask is usually 255.255.255.0.
- Default Gateway — the IP address of the router on your network. For example, in a network with a NETGEAR router, the gateway address is usually 192.168.0.1 or 192.168.1.1.

The Device Name is the NetBIOS name used by Windows networks. On Windows PCs, you may see the NetBIOS name for the wireless game adapter listed under Network Neighborhood. You can change the default Device Name on this screen if you like.

After changing the configuration, click the Save button to save the values permanently to the Wireless Game Adapter. If you click Cancel, no modifications will be made.

Changing the WGE111 Wireless Game Adapter Password

To change the WGE111 Wireless Game Adapter password from the Web browser configuration screen:

1. Click Change Password.
2. Type the old password in the Old Password box. The default password is password.
3. Type a new password in the New Password box.
4. Re-type the new password in the Confirm Password box.
5. Click Apply.

Upgrading the Firmware

If a firmware upgrade for the WGE111 Wireless Game Adapter becomes available, you can download the software from *http://www.netgear.com* to your computer and then use the browser-based configuration software to upgrade the wireless game adapter.

IMPORTANT! Do not try to go online, turn off the WGE111 Wireless Game Adapter, shut down the computer or do anything else to the wireless game adapter until it finishes restarting! When the LED indicator lights turn on, wait a few more seconds before doing anything with the wireless game adapter.

To upgrade the wireless game adapter software:

1. Select Upgrade Firmware.

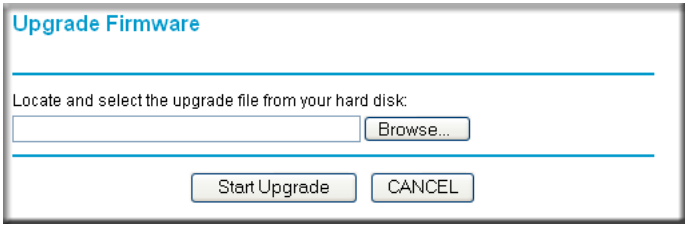


Figure 4-6: Upgrade Firmware screen

2. Click Browse and locate the downloaded software.
3. Click Start Upgrade.

4. After the firmware has been upgraded, you will need to log in to the router using your Web browser.

Restoring the Factory Defaults

You can use the Restore Factory Defaults screen to restore the wireless game adapter to the factory default settings.

Figure 4-7: Restore Factory Defaults screen

Click Restore to erase the current settings and reset the wireless game adapter to the original factory default settings.

IMPORTANT! Do not try to go online, turn off the wireless game adapter, shut down the computer or do anything else to the WGE111 Wireless Game Adapter until it finishes restarting! When the LED lights turns on, wait a few more seconds before doing anything with the WGE111 Wireless Game Adapter.

After you have erased the WGE111 Wireless Game Adapter's current settings, the adapter's password will be password, the LAN IP address will be 192.168.0.202 and the SSID will by default be ANY for Infrastructure mode and netgear for Ad-Hoc mode.

Chapter 5
Troubleshooting

This chapter gives information about troubleshooting your NETGEAR WGE111 Wireless Game Adapter. After each problem description, instructions are provided to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

If you have trouble setting up your WGE111, check the tips below. You can also consult more extensive troubleshooting procedures in the Reference Manual on the NETGEAR, Inc. Web site at *http://kbserver.netgear.com/products/wge111.asp*.

Note: The WGE111 can be used as a wireless game adapter with one machine only and does not support multiple devices.

- The wireless game adapter LEDs are not lit.

  Go to "Basic Tips" on page 5-2.

- I can't access the wireless game adapter from my computer.

  Go to "Troubleshooting the TCP/IP Settings Using Ping" on page 5-6.

- I can't access the Wireless Game Adapter configuration with my browser.

  Go to "Troubleshooting the Web Configuration Interface" on page 5-6.

- I can't remember the wireless game adapter's configuration password, or I want to clear the configuration and start over again.

  Go to "Restoring the Default Configuration and Password" on page 5-7.

Basic Tips

If you have problems connecting to your wireless network, try the tips below.

Symptom	Cause	Solution
The WGE111 Wireless Game Adapter has no power.	Power is not connected to the wireless game adapter.	• Make sure the power cord is connected to the wireless game adapter. • Make sure the power adapter is connected to a functioning power outlet. If it is in a power strip, make sure the power strip is turned on. If it is plugged directly into the wall, verify that it is not a switched outlet. • Make sure you are using the correct NETGEAR power adapter supplied with your wireless game adapter.
No lights are lit on the wireless game adapter	The WGE111 is starting up.	It takes a few seconds for the status light to be lit. Wait a minute and check the status light on the wireless game adapter.
The Internet light is solid but I cannot connect to the Internet.	There is a network configuration problem.	Make sure the wireless network security settings and the WGE111 security settings match. Make sure the PC, wireless game adapter, and router IP settings are correct.
The Internet LED blinks and cannot connect to an access point.	The WGE111 is attempting to connect to an access point, but cannot connect.	The access point may not be powered on. Or, the access point and the WGE111 are not configured with the same wireless parameters. Check the SSID and WEP settings. Make sure the WGE111 is within range of the wireless network.

My gaming console or remote computer cannot connect to the Internet.	There is a problem connecting to the wireless router.	• Make sure Internet light is on solidly. If not, see the previous symptom/solution. Make sure the gaming console or remote computer has a correct IP address with the same IP subnet address as the wireless router or access point. • Turn the wireless game adapter off and then back on. Recheck the IP address for the gaming console or remote computer. • Turn off all devices. Then, power on the wireless router (or access point), wait, and then power on the wireless game adapter. Check that the wireless game adapter connects to the wireless router or access point. If it connects, power on the gaming console or remote computer.
My computer cannot communicate with my wireless game adapter.	The most likely reason is a network configuration problem.	• Check that the wireless-enabled computer is on the same wireless network as the wireless game adapter. • Make sure the Network Name (SSID), WEP key (if WEP is enabled), and country/region selection are the same for all devices connected to the same wireless network. • If the computer is connected to the wireless game adapter through a switch or hub, try connecting it directly to the WGE111 Wireless Game Adapter.
I can't get the configuration utility to show the wireless game adapter. -or- I can't open the configuration software with my browser.	This could be a network configuration problem or a hardware connection problem.	• If the wireless LAN setting are correct, make sure all the devices are on the same IP network. • Make sure the Ethernet cable connectors are plugged into the computer and wireless game adapter securely. You may need to change the IP address of your computer temporarily to change the wireless game adapter's IP address. • Reset to factory defaults. **Note:** Some older Ethernet adapters may not be compatible with the Ethernet MAC address of the wireless game adapter.

I have a gaming console, computer, and the wireless game adapter connected through a switch. The computer connects to the Internet but the gaming console can't.	If using a switch or hub with an Ethernet-enabled gaming console, the gaming console must be powered on before the other Ethernet-enabled devices.	With power on, disconnect everything from the switch or hub. Re-connect the WGE111 Wireless Game Adapter, then connect the game console(s). Finally, connect the other device(s).
I can connect to an access point, but I cannot connect to other computers on the network or the Internet.	This could be a physical layer problem or a network configuration problem.	Check to make sure that the access point is physically connected to the Ethernet network. Make sure that the IP addresses and the Windows networking parameters are all configured correctly. Restart the cable or DSL modem, router, access point, and notebook PC.
I am using Ad-Hoc mode and my two WGE111 Wireless Game Adapters cannot connect.	This could be due to conflicting IP addresses.	Each WGE111 Wireless Game Adapter is factory-shipped with the IP address 192.168.0.202. You should not use the same IP address for more than one device on your network. Change the IP address of one of the adapters. See "Using the NETGEAR Smart Wizard Configuration Assistant" on page 3-9 for information on setting the IP address.

Frequently Asked Questions

Use the information below to solve common problems you may encounter. Also, please refer to the knowledge base on the NETGEAR Web site at *http://ww.netgear.com/support/main.asp*.

Note: For the most up-to-date WGE111 installation details and troubleshooting guidance visit *http://www.netgear.com*.

If you have trouble setting up your WGE111, check the tips below.

I am using a DHCP server, and the Wireless Game Adapter gets an IP address conflict.

If the wireless game adapter is left on when the DHCP server is turned off, the wireless game adapter will retain its IP Address without informing the DHCP server. Reset the wireless game adapter so it will obtain a new IP Address. This problem also arises if you assigned a static IP Address within the range used by the DHCP server. If so, use another address NOT within the range used by the DHCP server.

Be sure to observe the range and placement guidelines published in the Reference Manual.

I cannot configure the WGE111 from a browser.

You did not specify the correct wireless game adapter IP address, or there could be a system problem. Check the suggestions below and also see "Troubleshooting the Web Configuration Interface" on page 5-6.

- Remove and reconnect the power to the wireless game adapter.
- Make sure your computer and the wireless game adapter are in the same subnet. Both IP addresses should start with the same numbers. For example, 192.168.0.x. The subnet masks must match. For example, both should be 255.255.255.0.
- Enter the correct IP address in the address field of the browser. 192.168.0.202 is the WGE111 default IP address.

Troubleshooting the TCP/IP Settings Using Ping

The Windows ping utility sends an echo request packet to the designated device. The device then responds with an echo reply. You can ping the wireless game adapter from your computer to verify that the LAN path to your wireless game adapter is set up correctly.

To ping the wireless game adapter from a PC running Windows 95 or later:

1. From the Windows toolbar, click the Start button and select Run.
2. In the field provided, type Ping followed by the IP address of the wireless game adapter, as in this example:

   ping 192.168.0.202

3. Click OK.

   You should see a message like this one:

   Pinging <IP address> with 32 bytes of data

   If the path is working, you see this message:

   Reply from < IP address >: bytes=32 time=NN ms TTL=xxx

   If the path is not working, you see this message:

   Request timed out

   If the path is not functioning correctly, you could have one of the following problems:

   - Wrong physical connections
     - — Make sure the Status LED is on.
   - Wrong network configuration
     - — Verify that the IP address for your wireless game adapter and your workstation are correct and that the addresses are on the same subnet.

Troubleshooting the Web Configuration Interface

If you are unable to access the wireless game adapter's Web Configuration interface from a computer on your local network, check the following:

- Check the Ethernet connection between the computer and the wireless game adapter as described in the previous section.

- Make sure your computer's IP address is not shown as 169.254.x.x:
  Recent versions of Windows and Mac OS will generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the wireless game adapter and reboot your computer.
- If your wireless game adapter's IP address has been changed and you don't know the current IP address, clear the wireless game adapter's configuration to factory defaults. This will set the wireless game adapter's IP address to 192.168.0.202. This procedure is explained in "Restoring the Default Configuration and Password" on page 5-7.
- Try quitting the browser and launching it again.
- Make sure you are using the correct login information. The factory default password is **password**. Make sure that CAPS LOCK is off when entering this information.

If the wireless game adapter does not save changes you have made in the Web Configuration interface, check the following:

- When entering configuration settings, be sure to click the Apply button before moving to another menu or tab, or your changes are lost.
- Click the Refresh or Reload button in the Web browser. The changes may have occurred, but the Web browser may be caching the old configuration.

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, change the wireless game adapter's administration password to **password** and the IP address to 192.168.0.202. You can erase the current configuration and restore factory defaults in two ways:

- Use the Restore function of the Web Configuration Manager (see "Restoring the Factory Defaults" on page 4-12).
- Use the Default Reset button on the rear panel of the wireless game adapter. Use this method for cases when the administration password or IP address is not known. See "Reset Push Button" on page 2-5 for a description of this button.

Appendix A
Technical Specifications

This appendix provides technical specifications for the NETGEAR WGE111 Wireless Game Adapter.

Standards Compatibility	IEEE 802.3u, 100BASE-TX, Fast Ethernet IEEE 802.3i 10BASE-T CSMA/CD NetBEUI, and TCP/IP protocols
Data Rate	10/100 Mbps differential Manchester encoded
Interface	10BASE-T/100BASE-TX network port (RJ-45)
Power Specifications for the Power Adapter	Input voltage: 100 to 240 V AC, 50 to 60 Hz, according to the power adapter Localized plug: For North America, Japan, UK, Europe, and Australia Output voltage: 5 V DC at 2 A
Power Specifications for the Wireless Game Adapter	Power consumption: 5 W maximum Input voltage: 5 V DC at 2 Amps, maximum
Width	3.14 in (79.69 mm)
Height	4.72 in (120 mm)
Depth	1.19 in (3.25 mm)
Weight	132 g
Operating Temperature	0 to 40 C (32 to 104 F)
Operating Humidity	90% maximum relative humidity, noncondensing
Electromagnetic Emissions Compliance	CE mark, commercial FCC Part 15, Class A EN 55 022 (CISPR 22), Class A VCCI Class A ITE C-Tick N10947
Safety Agency Approvals, Power Adapter	CE mark, commercial UL listed (UL 1950) CSA certified (CSA 22.2 #950) TUV licensed (EN 60 950) T-Mark

Appendix B
Understanding IP Addresses

This appendix provides information about understanding IP addresses, which you must assign to the NETGEAR WGE111 Wireless Game Adapter when operating in a TCP/IP environment.

IP Addresses and the Internet

Because TCP/IP networks are interconnected across the world, every machine on the Internet must have a unique address to make sure that transmitted data reaches the correct destination. Blocks of addresses are assigned to organizations by the Internet Assigned Numbers Authority (IANA). Individual users and small organizations may obtain their addresses either from the IANA or from an Internet service provider (ISP). You can contact IANA at www.iana.org.

The Internet Protocol (IP) uses a 32-bit address structure. The address is usually written in dot notation (also called dotted-decimal notation), in which each group of eight bits is written in decimal form, separated by decimal points.

For example, the following binary address:

```
11000011  00100010  00001100  00000111
```

is normally written as:

```
195.34.12.7
```

The latter version is easier to remember and easier to enter into your computer.

In addition, the 32 bits of the address are subdivided into two parts. The first part of the address identifies the network, and the second part identifies the host node or station on the network. The dividing point may vary depending on the address range and the application.

There are five standard classes of IP addresses. These address classes have different ways of determining the network and host sections of the address, allowing for different numbers of hosts on a network. Each address type begins with a unique bit pattern, which is used by the TCP/IP software to identify the address class. After the address class has been determined, the software can correctly identify the host section of the address. The follow figure shows the three main address classes, including network and host sections of the address for each address type.

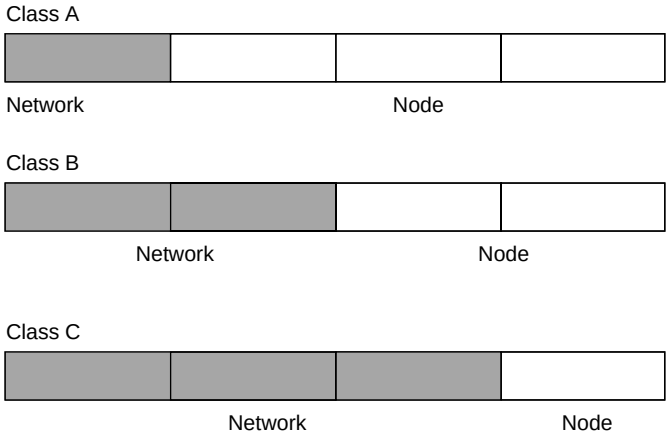


Figure 5-1: Three Main Address Classes

The five address classes are:

- Class A
  Class A addresses can have up to 16,777,214 hosts on a single network. They use an eight-bit network number and a 24-bit node number. Class A addresses are in this range:

  1.x.x.x to 126.x.x.x.

- Class B
  Class B addresses can have up to 65,354 hosts on a network. A Class B address uses a 16-bit network number and a 16-bit node number. Class B addresses are in this range:

  128.1.x.x to 191.254.x.x.

- Class C
  Class C addresses can have 254 hosts on a network. Class C addresses use 24 bits for the network address and eight bits for the node. They are in this range:

  192.0.1.x to 223.255.254.x.

- Class D
  Class D addresses are used for multicasts (messages sent to many hosts). Class D addresses are in this range:

  224.0.0.0 to 239.255.255.255.

- Class E
  Class E addresses are for experimental use.

This addressing structure allows IP addresses to uniquely identify each physical network and each node on each physical network.

For each unique value of the network portion of the address, the base address of the range (host address of all zeros) is known as the network address and is not usually assigned to a host. Also, the top address of the range (host address of all ones) is not assigned, but is used as the broadcast address for simultaneously sending a packet to all hosts with the same network address.

Netmask

In each of the address classes previously described, the size of the two parts (network address and host address) is implied by the class. This partitioning scheme can also be expressed by a netmask associated with the IP address. A netmask is a 32-bit quantity that, when logically combined (using an AND operator) with an IP address, yields the network address. For instance, the netmasks for Class A, B, and C addresses are 255.0.0.0, 255.255.0.0, and 255.255.255.0, respectively.

For example, the address 192.168.170.237 is a Class C IP address whose network portion is the upper 24 bits. When combined (using an AND operator) with the Class C netmask, as shown here, only the network portion of the address remains:

```
11000000  10101000  10101010  11101101 (192.168.170.237)
```

combined with:

```
11111111  11111111  11111111  00000000 (255.255.255.0)
```

Equals:

```
11000000  10101000  10101010  00000000 (192.168.170.0)
```

As a shorter alternative to dotted-decimal notation, the netmask may also be expressed in terms of the number of ones from the left. This number is appended to the IP address, following a backward slash (/), as “/n.” In the example, the address could be written as 192.168.170.237/24, indicating that the netmask is 24 ones followed by 8 zeros.

Subnet Addressing

By looking at the addressing structures, you can see that even with a Class C address, there are a large number of hosts per network. Such a structure is an inefficient use of addresses if each end of a routed link requires a different network number. It is unlikely that the smaller office LANs would have that many devices. You can resolve this problem by using a technique known as subnet addressing.

Subnet addressing allows us to split one IP network address into smaller multiple physical networks known as subnetworks. Some of the node numbers are used as a subnet number instead. A Class B address gives us 16 bits of node numbers translating to 64,000 nodes. Most organizations do not use 64,000 nodes, so there are free bits that can be reassigned. Subnet addressing makes use of those bits that are free, as shown below.

Figure 5-2: Example of Subnetting a Class B Address

A Class B address can be effectively translated into multiple Class C addresses. For example, the IP address of 172.16.0.0 is assigned, but node addresses are limited to 255 maximum, allowing eight extra bits to use as a subnet address. The IP address of 172.16.97.235 would be interpreted as IP network address 172.16, subnet number 97, and node number 235. In addition to extending the number of addresses available, subnet addressing provides other benefits. Subnet addressing allows a network manager to construct an address scheme for the network by using different subnets for other geographical locations in the network or for other departments in the organization.

Although the preceding example uses the entire third octet for a subnet address, note that you are not restricted to octet boundaries in subnetting. To create more network numbers, you need only shift some bits from the host address to the network address. For instance, to partition a Class C network number (192.68.135.0) into two, you shift one bit from the host address to the network address. The new netmask (or subnet mask) is 255.255.255.128. The first subnet has network number 192.68.135.0 with hosts 192.68.135.1 to 129.68.135.126, and the second subnet has network number 192.68.135.128 with hosts 192.68.135.129 to 192.68.135.254.

Note: The number 192.68.135.127 is not assigned because it is the broadcast address of the first subnet. The number 192.68.135.128 is not assigned because it is the network address of the second subnet.

The following table lists the additional subnet mask bits in dotted-decimal notation. To use the table, write down the original class netmask and replace the 0 value octets with the dotted-decimal value of the additional subnet bits. For example, to partition your Class C network with subnet mask 255.255.255.0 into 16 subnets (4 bits), the new subnet mask becomes 255.255.255.240.

Table 5-1. Netmask Notation Translation Table for One Octet

Number of Bits	Dotted-Decimal Value
1	128
2	192
3	224
4	240
5	248
6	252
7	254
8	255

The following table displays several common netmask values in both the dotted-decimal and the masklength formats.

Table 5-2. Netmask Formats

Dotted-Decimal	Masklength
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29

Table 5-2. Netmask Formats

255.255.255.252	/30
255.255.255.254	/31
255.255.255.255	/32

NETGEAR strongly recommends that you configure all hosts on a LAN segment to use the same netmask for the following reasons:

- So that hosts recognize local IP broadcast packets.

  When a device broadcasts to its segment neighbors, it uses a destination address of the local network address with all ones for the host address. In order for this scheme to work, all devices on the segment must agree on which bits comprise the host address.

- So that a local router or bridge recognizes which addresses are local and which are remote.

Private IP Addresses

If your networks are isolated from the Internet (for example, only between your two branch offices), you can assign any IP addresses to the hosts without problems. However, the IANA has reserved the following three blocks of IP addresses specifically for private networks:

```
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255
```

NETGEAR recommends that you choose your private network number from this range. NETGEAR products default to 192.168.0.xxx or 192.168.1.1.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines explained here. For more information about address assignment, refer to RFC 1597, *Address Allocation for Private Internets*, and RFC 1466, *Guidelines for Management of IP Address Space*. The Internet Engineering Task Force (IETF) publishes RFCs on its Web site at *www.ietf.org*.

Address Resolution Protocol

An IP address alone cannot be used to deliver data from one device to another on a LAN. In order for data to be sent from one device on the LAN to another, you must convert the IP address of the destination device to its media access control (MAC) address. Each device on an Ethernet network has a unique Ethernet MAC address, which is a 48-bit number assigned to each device by the manufacturer. The technique that associates the IP address with a MAC address is known as address resolution, and IP uses the Address Resolution Protocol (ARP) to do this.

If a device needs to send data to another station on the network and it does not already have the destination MAC address recorded, ARP is used. An ARP request is broadcast onto the network, and all stations receive and read the request. The destination IP address is included as part of the message so that only the station with the correct IP address responds to the ARP request and all other nodes discard it.

The node with the right IP address responds with its own MAC address directly to the sender, providing the transmitting station with the destination MAC address needed for it to send the data. The IP address data and MAC address data for each node are held in an ARP table, so that the next time data needs to be sent, the address can be obtained from the address information in the table.

IP Configuration by DHCP

When an IP-based local area network is installed, each workstation must be configured with an IP address. If the workstations need to access the Internet, they should also be configured with a gateway address and one or more DNS server addresses. As an alternative to manual configuration, there is a method by which each device on the network can obtain this configuration information automatically. A device on the network may act as a Dynamic Host Configuration Protocol (DHCP) server. The DHCP server stores a list or pool of IP addresses, along with other information (such as gateway and DNS addresses) that it may assign to the other devices on the network. The most of NETGEAR routers have the capacity to act as a DHCP server.

Appendix C
Wireless Networking Basics

This chapter provides an overview of wireless networking.

Wireless Networking Overview

On an 802.11b or g wireless link, data is encoded using direct-sequence spread-spectrum (DSSS) technology and is transmitted in the unlicensed radio spectrum at 2.5GHz. The maximum data rate for the wireless link is 11 Mbps, but it will automatically back down from 11 Mbps to 5.5, 2, and 1 Mbps when the radio signal is weak or when interference is detected. The 802.11g auto rate sensing rates are 1, 2, 5.5, 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

The 802.11 standard is also called Wireless Ethernet or Wi-Fi by the Wireless Ethernet Compatibility Alliance (WECA, see *http://www.wi-fi.net*), an industry standard group promoting interoperability among 802.11 devices. The 802.11 standard offers two methods for configuring a wireless network — ad hoc and infrastructure.

Infrastructure Mode

With a wireless access point, you can operate the wireless LAN in the infrastructure mode. This mode provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage, interacting with wireless nodes via an antenna.

In the infrastructure mode, the wireless access point converts airwave data into wired Ethernet data, acting as a bridge between the wired LAN and wireless clients. Connecting multiple access points via a wired Ethernet backbone can further extend the wireless network coverage. As a mobile computing device moves out of the range of one access point, it moves into the range of another. As a result, wireless clients can freely roam from one access point domain to another and still maintain seamless network connection.

Ad Hoc Mode (Peer-to-Peer Workgroup)

In an ad hoc network, computers are brought together as needed; thus, there is no structure or fixed points to the network — each node can generally communicate with any other node. There is no access point involved in this configuration. This mode enables you to quickly set up a small wireless workgroup and allows workgroup members to exchange data or share printers as supported by Microsoft networking in the various Windows operating systems. Some vendors also refer to ad hoc networking as peer-to-peer group networking.

In this configuration, network packets are directly sent and received by the intended transmitting and receiving stations. As long as the stations are within range of one another, this is the easiest and least expensive way to set up a wireless network.

Network Name: Extended Service Set Identification (ESSID)

The Extended Service Set Identification (ESSID) is one of two types of Service Set Identification (SSID). In an ad hoc wireless network with no access points, the Basic Service Set Identification (BSSID) is used. In an infrastructure wireless network that includes an access point, the ESSID is used, but may still be referred to as SSID.

An SSID is a thirty-two character (maximum) alphanumeric key identifying the name of the wireless local area network. Some vendors refer to the SSID as network name. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID.

Authentication and WEP

The absence of a physical connection between nodes makes the wireless links vulnerable to eavesdropping and information theft. To provide a certain level of security, the IEEE 802.11 standard has defined two types of authentication methods, Open System and Shared Key. With Open System authentication, a wireless PC can join any network and receive any messages that are not encrypted. With Shared Key authentication, only those PCs that possess the correct authentication key can join the network. By default, IEEE 802.11 wireless devices operate in an Open System network.

Wired Equivalent Privacy (WEP) data encryption is used when the wireless devices are configured to operate in Shared Key authentication mode. There are two shared key methods implemented in most commercially available products, 64-bit and 128-bit WEP data encryption.

802.11 Authentication

The 802.11 standard defines several services that govern how two 802.11 devices communicate. The following events must occur before an 802.11 Station can communicate with an Ethernet network through an access point such as the one built in to the WG511:

1. Turn on the wireless station.
2. The station listens for messages from any access points that are in range.
3. The station finds a message from an access point that has a matching SSID.
4. The station sends an authentication request to the access point.
5. The access point authenticates the station.
6. The station sends an association request to the access point.
7. The access point associates with the station.
8. The station can now communicate with the Ethernet network through the access point.

An access point must authenticate a station before the station can associate with the access point or communicate with the network. The IEEE 802.11 standard defines two types of authentication: Open System and Shared Key.

- Open System Authentication allows any device to join the network, assuming that the device SSID matches the access point SSID. Alternatively, the device can use the “ANY” SSID option to associate with any available access point within range, regardless of its SSID.
- Shared Key Authentication requires that the station and the access point have the same WEP Key to authenticate. These two authentication procedures are described below.

Open System Authentication

The following steps occur when two devices use Open System Authentication:

1. The station sends an authentication request to the access point.
2. The access point authenticates the station.
3. The station associates with the access point and joins the network.

This process is illustrated below.

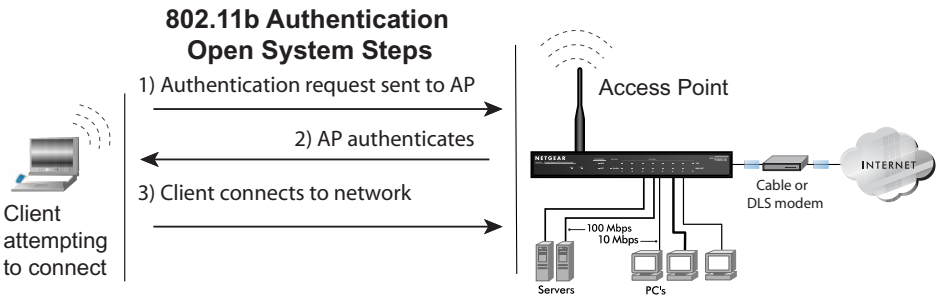


Figure C-1: 802.11 open system authentication

Shared Key Authentication

The following steps occur when two devices use Shared Key Authentication:

1. The station sends an authentication request to the access point.
2. The access point sends challenge text to the station.
3. The station uses its configured 64-bit or 128-bit default key to encrypt the challenge text, and sends the encrypted text to the access point.
4. The access point decrypts the encrypted text using its configured WEP key that corresponds to the station's default key. The access point compares the decrypted text with the original challenge text. If the decrypted text matches the original challenge text, then the access point and the station share the same WEP key and the access point authenticates the station.
5. The station connects to the network.

If the decrypted text does not match the original challenge text (i.e., the access point and station do not share the same WEP key), then the access point will refuse to authenticate the station and the station will be unable to communicate with either the 802.11 network or Ethernet network.

This process is illustrated below.

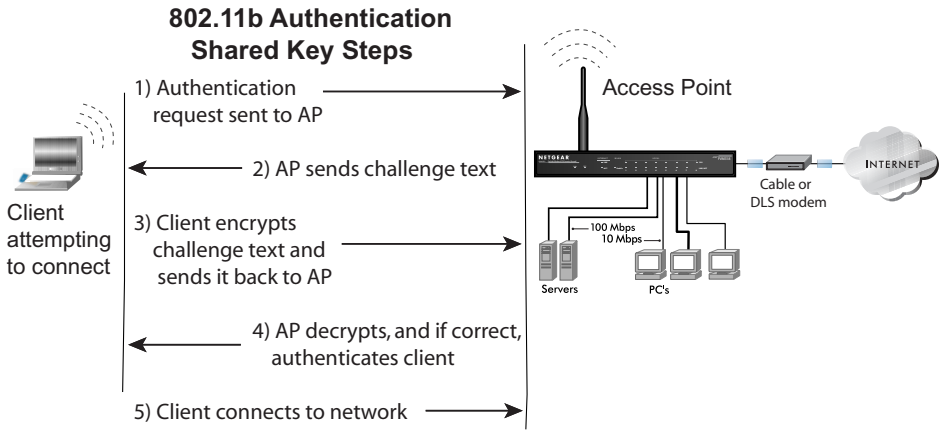


Figure C-2: 802.11 shared key authentication

Overview of WEP Parameters

Before enabling WEP on an 802.11 network, you must first consider what type of encryption you require and the key size you want to use. Typically, there are three WEP Encryption options available for 802.11 products:

1. **Do Not Use WEP:** The 802.11 network does not encrypt data. For authentication purposes, the network uses Open System Authentication.

2. **Use WEP for Encryption:** A transmitting 802.11 device encrypts the data portion of every packet it sends using a configured WEP key. The receiving 802.11b device decrypts the data using the same WEP key. For authentication purposes, the 802.11b network uses Open System Authentication.

3. **Use WEP for Authentication and Encryption:** A transmitting 802.11 device encrypts the data portion of every packet it sends using a configured WEP key. The receiving 802.11 device decrypts the data using the same WEP key. For authentication purposes, the 802.11 network uses Shared Key Authentication.

Note: Some 802.11 access points also support **Use WEP for Authentication Only** (Shared Key Authentication without data encryption).

Key Size

The IEEE 802.11 standard supports two types of WEP encryption: 40-bit and 128-bit.

The 64-bit WEP data encryption method, allows for a five-character (40-bit) input. Additionally, 24 factory-set bits are added to the forty-bit input to generate a 64-bit encryption key. (The 24 factory-set bits are not user-configurable). This encryption key will be used to encrypt/decrypt all data transmitted via the wireless interface. Some vendors refer to the 64-bit WEP data encryption as 40-bit WEP data encryption since the user-configurable portion of the encryption key is 40 bits wide.

The 128-bit WEP data encryption method consists of 104 user-configurable bits. Similar to the forty-bit WEP data encryption method, the remaining 24 bits are factory set and not user configurable. Some vendors allow passphrases to be entered instead of the cryptic hexadecimal characters to ease encryption key entry.

128-bit encryption is stronger than 40-bit encryption, but 128-bit encryption may not be available outside of the United States due to U.S. export regulations.

When configured for 40-bit encryption, 802.11 products typically support up to four WEP keys. Each 40-bit WEP key is expressed as 5 sets of two hexadecimal digits (0-9 and A-F). For example, “12 34 56 78 90” is a 40-bit WEP key.

When configured for 128-bit encryption, 802.11b products typically support four WEP keys but some manufacturers support only one 128-bit key. The 128-bit WEP key is expressed as 13 sets of two hexadecimal digits (0-9 and A-F). For example, “12 34 56 78 90 AB CD EF 12 34 56 78 90” is a 128-bit WEP key.

Note: Typically, 802.11 access points can store up to four 128-bit WEP keys but some 802.11 client adapters can only store one. Therefore, make sure that your 802.11 access and client adapters configurations match.

WEP Configuration Options

The WEP settings must match on all 802.11 devices that are within the same wireless network as identified by the SSID. In general, if your mobile clients will roam between access points, then all of the 802.11 access points and all of the 802.11 client adapters on the network must have the same WEP settings.

Note: Whatever keys you enter for an AP, you must also enter the same keys for the client adapter in the same order. In other words, WEP key 1 on the AP must match WEP key 1 on the client adapter, WEP key 2 on the AP must match WEP key 2 on the client adapter, etc.

Note: The AP and the client adapters can have different default WEP keys as long as the keys are in the same order. In other words, the AP can use WEP key 2 as its default key to transmit while a client adapter can use WEP key 3 as its default key to transmit. The two devices will communicate as long as the AP's WEP key 2 is the same as the client's WEP key 2 and the AP's WEP key 3 is the same as the client's WEP key 3.

Wireless Channels

IEEE 802.11b and g wireless nodes communicate with each other using radio frequency signals in the ISM (Industrial, Scientific, and Medical) band between 2.4 GHz and 2.5 GHz. Neighboring channels are 5 MHz apart. However, due to spread spectrum effect of the signals, a node sending signals using a particular channel will utilize frequency spectrum 12.5 MHz above and below the center channel frequency. As a result, two separate wireless networks using neighboring channels (for example, channel 1 and channel 2) in the same general vicinity will interfere with each other. Applying two channels that allow the maximum channel separation will decrease the amount of channel cross-talk, and provide a noticeable performance increase over networks with minimal channel separation.

The radio frequency channels used are listed in the table below:

Table C-1. 802.11b and g Radio Frequency Channels

Channel	Center Frequency	Frequency Spread
1	2412 MHz	2399.5 MHz - 2424.5 MHz
2	2417 MHz	2404.5 MHz - 2429.5 MHz
3	2422 MHz	2409.5 MHz - 2434.5 MHz
4	2427 MHz	2414.5 MHz - 2439.5 MHz
5	2432 MHz	2419.5 MHz - 2444.5 MHz
6	2437 MHz	2424.5 MHz - 2449.5 MHz
7	2442 MHz	2429.5 MHz - 2454.5 MHz
8	2447 MHz	2434.5 MHz - 2459.5 MHz
9	2452 MHz	2439.5 MHz - 2464.5 MHz
10	2457 MHz	2444.5 MHz - 2469.5 MHz
11	2462 MHz	2449.5 MHz - 2474.5 MHz
12	2467 MHz	2454.5 MHz - 2479.5 MHz
13	2472 MHz	2459.5 MHz - 2484.5 MHz

Note: The available channels supported by the wireless products in various countries are different.

The preferred channel separation between the channels in neighboring wireless networks is 25 MHz (5 channels). This means that you can apply up to three different channels within your wireless network. There are only 11 usable wireless channels in the United States. It is recommended that you start using channel 1 and grow to use channel 6, and 11 when necessary, as these three channels do not overlap.

WPA Wireless Security

Wi-Fi Protected Access (WPA) is a specification of standards-based, interoperable security enhancements that increase the level of data protection and access control for existing and future wireless LAN systems.

The IEEE introduced the WEP as an optional security measure to secure 802.11b (Wi-Fi) WLANs, but inherent weaknesses in the standard soon became obvious. In response to this situation, the Wi-Fi Alliance announced a new security architecture in October 2002 that remedies the shortcomings of WEP. This standard, formerly known as Safe Secure Network (SSN), is designed to work with existing 802.11 products and offers forward compatibility with 802.11i, the new wireless security architecture being defined in the IEEE.

WPA offers the following benefits:

- Enhanced data privacy
- Robust key management
- Data origin authentication
- Data integrity protection

How Does WPA Compare to WEP?

WEP is a data encryption method and is not intended as a user authentication mechanism. WPA user authentication is implemented using 802.1x and the Extensible Authentication Protocol (EAP). Support for 802.1x authentication is required in WPA. In the 802.11 standard, 802.1x authentication was optional. For details on EAP specifically, refer to IETF's RFC 2284.

With 802.11 WEP, all access points and client wireless adapters on a particular wireless LAN must use the same encryption key. A major problem with the 802.11 standard is that the keys are cumbersome to change. If you do not update the WEP keys often, an unauthorized person with a sniffing tool can monitor your network for less than a day and decode the encrypted messages. Products based on the 802.11 standard alone offer system administrators no effective method to update the keys.

For 802.11, WEP encryption is optional. For WPA, encryption using Temporal Key Integrity Protocol (TKIP) is required. TKIP replaces WEP with a new encryption algorithm that is stronger than the WEP algorithm, but that uses the calculation facilities present on existing wireless devices to perform encryption operations. TKIP provides important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. Through these enhancements, TKIP addresses all of known WEP vulnerabilities.

How Does WPA Compare to IEEE 802.11i?

WPA is a subset of the current 802.11i draft and uses certain pieces of the 802.11i draft that are ready to bring to market today, such as 802.1x and TKIP. The main pieces of the 802.11i draft that are not included in WPA are secure IBSS (Ad Hoc mode), secure fast handoff (for specialized 802.11 VoIP phones), as well as enhanced encryption protocols, such as AES-CCMP. These features are either not yet ready for market or will require hardware upgrades to implement.

What are the Key Features of WPA Security?

The following security features are included in the WPA standard:

- WPA Authentication
- WPA Encryption Key Management
  - Temporal Key Integrity Protocol (TKIP)
  - Michael message integrity code (MIC)
  - AES Support (to be phased in)
- Support for a Mixture of WPA and WEP Wireless Clients, but mixing WEP and WPA is discouraged

These features are discussed below.

WPA addresses most of the known WEP vulnerabilities and is primarily intended for wireless infrastructure networks as found in the enterprise. This infrastructure includes stations, access points, and authentication servers (typically RADIUS servers). The RADIUS server holds (or has access to) user credentials (for example, user names and passwords) and authenticates wireless users before they gain access to the network.

The strength of WPA comes from an integrated sequence of operations that encompass 802.1X/ EAP authentication and sophisticated key management and encryption techniques. Its major operations include:

- Network security capability determination. This occurs at the 802.11 level and is communicated through WPA information elements in Beacon, Probe Response, and (Re) Association Requests. Information in these elements includes the authentication method (802.1X or Pre-shared key) and the preferred cipher suite (WEP, TKIP, or AES).

The primary information conveyed in the Beacon frames is the authentication method and the cipher suite. Possible authentication methods include 802.1X and Pre-shared key. Pre-shared key is an authentication method that uses a statically configured passphrase on both the stations and the access point. This obviates the need for an authentication server, which in many home and small office environments will not be available nor desirable. Possible cipher suites include: WEP, TKIP, and AES (Advanced Encryption Standard). We talk more about TKIP and AES when addressing data privacy below.

- Authentication. EAP over 802.1X is used for authentication. Mutual authentication is gained by choosing an EAP type supporting this feature and is required by WPA. 802.1X port access control prevents full access to the network until authentication completes. 802.1X EAPOL-Key packets are used by WPA to distribute per-session keys to those stations successfully authenticated.

  The supplicant in the station uses the authentication and cipher suite information contained in the information elements to decide which authentication method and cipher suite to use. For example, if the access point is using the pre-shared key method then the supplicant need not authenticate using full-blown 802.1X. Rather, the supplicant must simply prove to the access point that it is in possession of the pre-shared key. If the supplicant detects that the service set does not contain a WPA information element then it knows it must use pre-WPA 802.1X authentication and key management in order to access the network.

- Key management. WPA features a robust key generation/management system that integrates the authentication and data privacy functions. Keys are generated after successful authentication and through a subsequent 4-way handshake between the station and access point.

- Data Privacy (Encryption). Temporal Key Integrity Protocol (TKIP) is used to wrap WEP in sophisticated cryptographic and security techniques to overcome most of its weaknesses.

- Data integrity. TKIP includes a message integrity code (MIC) at the end of each plain text message to ensure messages are not being spoofed.

WPA Authentication: Enterprise-level User Authentication via 802.1x/EAP and RADIUS

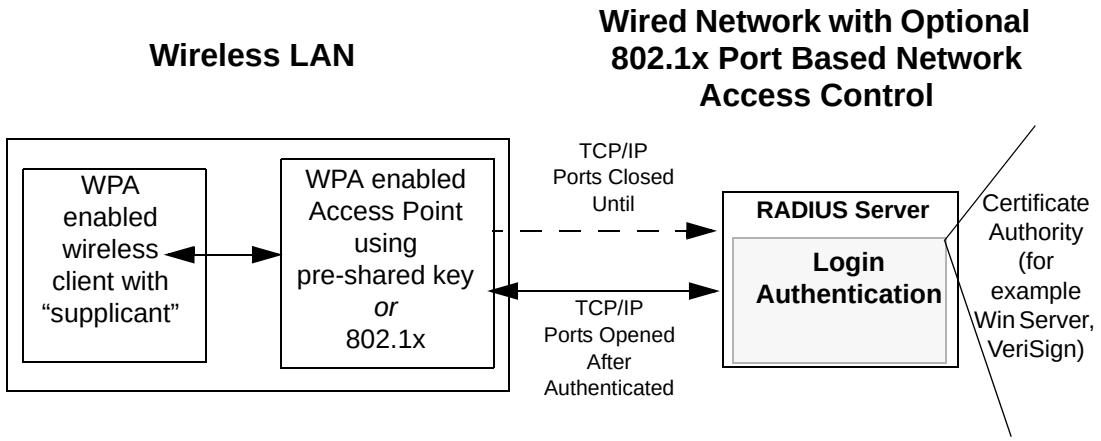


Figure C-3: WPA Overview

IEEE 802.1x offers an effective framework for authenticating and controlling user traffic to a protected network, as well as providing a vehicle for dynamically varying data encryption keys via EAP from a RADIUS server, for example. This framework enables using a central authentication server, which employs mutual authentication so that a rogue wireless user does not join the network.

It is important to note that 802.1x does not provide the actual authentication mechanisms. When using 802.1x, the EAP type, such as Transport Layer Security (EAP-TLS), or EAP Tunneled Transport Layer Security (EAP-TTLS), defines how the authentication takes place.

Note: For environments with a Remote Authentication Dial-In User Service (RADIUS) infrastructure, WPA supports Extensible Authentication Protocol (EAP). For environments without a RADIUS infrastructure, WPA supports the use of a pre-shared key.

Together, these technologies provide a framework for strong user authentication.

Windows XP implements 802.1x natively, and several NETGEAR switch and wireless access point products support 802.1x.

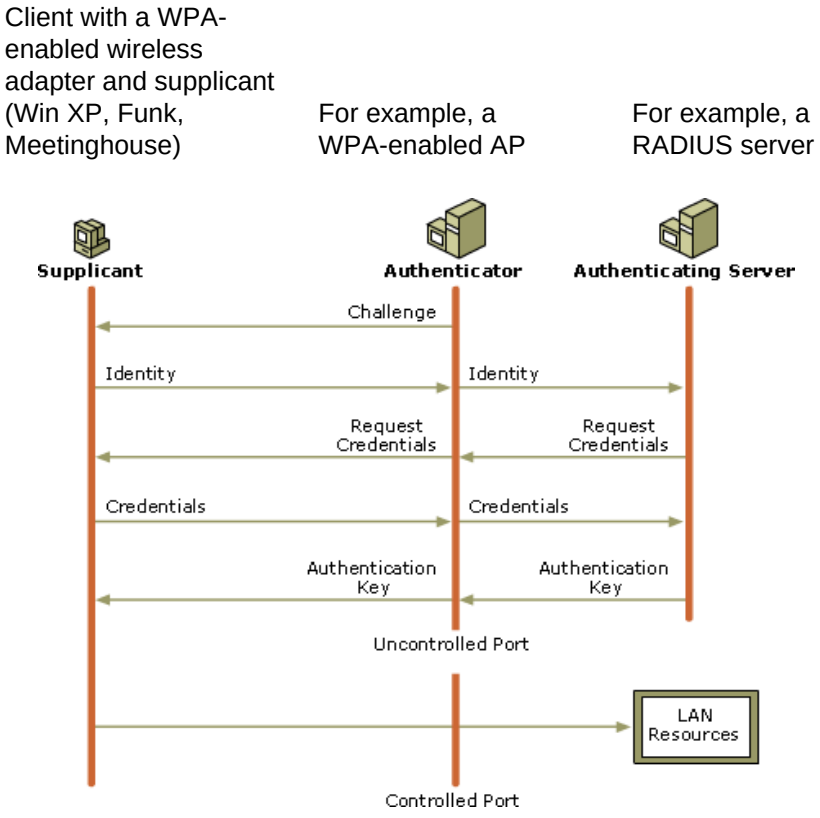


Figure C-4: 802.1x Authentication Sequence

The access point sends Beacon Frames with WPA information elements to the stations in the service set. Information elements include the required authentication method (802.1x or Pre-shared key) and the preferred cipher suite (WEP, TKIP, or AES). Probe Responses (AP to station) and Association Requests (station to AP) also contain WPA information elements.

1. Initial 802.1x communications begin with an unauthenticated supplicant (client device) attempting to connect with an authenticator (802.11 access point). The client sends an EAP-start message. This begins a series of message exchanges to authenticate the client.
2. The access point replies with an EAP-request identity message.

3. The client sends an EAP-response packet containing the identity to the authentication server. The access point responds by enabling a port for passing only EAP packets from the client to an authentication server located on the wired side of the access point. The access point blocks all other traffic, such as HTTP, DHCP, and POP3 packets, until the access point can verify the client's identity using an authentication server (for example, RADIUS).
4. The authentication server uses a specific authentication algorithm to verify the client's identity. This could be through the use of digital certificates or some other EAP authentication type.
5. The authentication server will either send an accept or reject message to the access point.
6. The access point sends an EAP-success packet (or reject packet) to the client.
7. If the authentication server accepts the client, then the access point will transition the client's port to an authorized state and forward additional traffic.

The important part to know at this point is that the software supporting the specific EAP type resides on the authentication server and within the operating system or application “supplicant” software on the client devices. The access point acts as a “pass through” for 802.1x messages, which means that you can specify any EAP type without needing to upgrade an 802.1x-compliant access point. As a result, you can update the EAP authentication type to such devices as token cards (Smart Cards), Kerberos, one-time passwords, certificates, and public key authentication, or as newer types become available and your requirements for security change.

WPA Data Encryption Key Management

With 802.1x, the rekeying of unicast encryption keys is optional. Additionally, 802.11 and 802.1x provide no mechanism to change the global encryption key used for multicast and broadcast traffic. With WPA, rekeying of both unicast and global encryption keys is required.

For the unicast encryption key, the Temporal Key Integrity Protocol (TKIP) changes the key for every frame, and the change is synchronized between the wireless client and the wireless access point (AP). For the global encryption key, WPA includes a facility (the Information Element) for the wireless AP to advertise the changed key to the connected wireless clients.

If configured to implement dynamic key exchange, the 802.1x authentication server can return session keys to the access point along with the accept message. The access point uses the session keys to build, sign and encrypt an EAP key message that is sent to the client immediately after sending the success message. The client can then use contents of the key message to define applicable encryption keys. In typical 802.1x implementations, the client can automatically change encryption keys as often as necessary to minimize the possibility of eavesdroppers having enough time to crack the key in current use.

Temporal Key Integrity Protocol (TKIP)

WPA uses TKIP to provide important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. TKIP also provides for the following:

- The verification of the security configuration after the encryption keys are determined.
- The synchronized changing of the unicast encryption key for each frame.
- The determination of a unique starting unicast encryption key for each preshared key authentication.

Michael

With 802.11 and WEP, data integrity is provided by a 32-bit *integrity check value* (ICV) that is appended to the 802.11 payload and encrypted with WEP. Although the ICV is encrypted, you can use cryptanalysis to change bits in the encrypted payload and update the encrypted ICV without being detected by the receiver.

With WPA, a method known as *Michael* specifies a new algorithm that calculates an 8-byte message integrity check (MIC) using the calculation facilities available on existing wireless devices. The MIC is placed between the data portion of the IEEE 802.11 frame and the 4-byte ICV. The MIC field is encrypted together with the frame data and the ICV.

Michael also provides replay protection. A new frame counter in the IEEE 802.11 frame is used to prevent replay attacks.

Optional AES Support to be Phased In

One of the encryption methods supported by WPA, besides TKIP, is the advanced encryption standard (AES), although AES support will not be required initially for Wi-Fi certification. This is viewed as the optimal choice for security conscience organizations, but the problem with AES is that it requires a fundamental redesign of the NIC's hardware in both the station and the access point. TKIP is a pragmatic compromise that allows organizations to deploy better security while AES capable equipment is being designed, manufactured, and incrementally deployed.

Is WPA Perfect?

WPA is not without its vulnerabilities. Specifically, it is susceptible to denial of service (DoS) attacks. If the access point receives two data packets that fail the message integrity code (MIC) within 60 seconds of each other, then the network is under an active attack, and as a result, the access point employs counter measures, which include disassociating each station using the access point. This prevents an attacker from gleaning information about the encryption key and alerts administrators, but it also causes users to lose network connectivity for 60 seconds. More than anything else, this may just prove that no single security tactic is completely invulnerable. WPA is a definite step forward in WLAN security over WEP and has to be thought of as a single part of an end-to-end network security strategy.

Product Support for WPA

WPA requires software changes to the following:

- Wireless access points
- Wireless network adapters
- Wireless client programs

Supporting a Mixture of WPA and WEP Wireless Clients is Discouraged

To support the gradual transition of WEP-based wireless networks to WPA, a wireless AP can support both WEP and WPA clients at the same time. During the association, the wireless AP determines which clients use WEP and which clients use WPA. The disadvantage to supporting a mixture of WEP and WPA clients is that the global encryption key is not dynamic. This is because WEP-based clients cannot support it. All other benefits to the WPA clients, such as integrity, are maintained.

However, a mixed mode supporting WPA and non-WPA clients would offer network security that is no better than that obtained with a non-WPA network, and thus this mode of operation is discouraged.

Changes to Wireless Access Points

Wireless access points must have their firmware updated to support the following:

- **The new WPA information element**
  To advertise their support of WPA, wireless APs send the beacon frame with a new 802.11 WPA information element that contains the wireless AP's security configuration (encryption algorithms and wireless security configuration information).
- **The WPA two-phase authentication**
  Open system, then 802.1x (EAP with RADIUS or preshared key).
- **TKIP**
- **Michael**
- **AES** (optional)

To upgrade your wireless access points to support WPA, obtain a WPA firmware update from your wireless AP vendor and upload it to your wireless AP.

Changes to Wireless Network Adapters

Wireless networking software in the adapter, and possibly in the OS or client application, must be updated to support the following:

- **The new WPA information element**
  Wireless clients must be able to process the WPA information element and respond with a specific security configuration.
- **The WPA two-phase authentication**
  Open system, then 802.1x supplicant (EAP or preshared key).
- **TKIP**
- **Michael**
- **AES** (optional)

To upgrade your wireless network adapters to support WPA, obtain a WPA update from your wireless network adapter vendor and update the wireless network adapter driver.

For Windows wireless clients, you must obtain an updated network adapter driver that supports WPA. For wireless network adapter drivers that are compatible with Windows XP (Service Pack 1) and Windows Server 2003, the updated network adapter driver must be able to pass the adapter's WPA capabilities and security configuration to the Wireless Zero Configuration service.

Microsoft has worked with many wireless vendors to embed the WPA firmware update in the wireless adapter driver. So, to update your Microsoft Windows wireless client, all you have to do is obtain the new WPA-compatible driver and install the driver. The firmware is automatically updated when the wireless network adapter driver is loaded in Windows.

Changes to Wireless Client Programs

Wireless client programs must be updated to permit the configuration of WPA authentication (and preshared key) and the new WPA encryption algorithms (TKIP and the optional AES component).

To obtain the Microsoft WPA client program, visit the Microsoft Web site.

Glossary

List of Glossary Terms

Use the list below to find definitions for technical terms used in this manual.

10BASE-T
IEEE 802.3 specification for 10 Mbps Ethernet over Category 3, 4, or 5 twisted pair wiring.

100BASE-Tx
IEEE 802.3 specification for 100 Mbps Fast Ethernet over Category 5 twisted pair wiring.

1000BASE-T

IEEE 802.3 specification for 1000 Mbps Gigabit Ethernet over Category 5 twisted pair wiring.

802.1Q

IEEE specification for the operation of Virtual LAN (VLAN) Bridges that permit the definition, operation and administration of Virtual LAN topologies within a Bridged LAN infrastructure.

802.3

The IEEE standard defining the hardware layer and transport layer of (a variant of) Ethernet. The maximum segment length is 500m and the maximum total length is 2.5km. The maximum number of hosts is 1024. The maximum packet size is 1518 bytes.

802.3ab

Gigabit ethernet over Copper (also known as 1000BaseT) is an extension of the existing Fast Ethernet standard. It specifies Gigabit Ethernet operation over the Category 5e/6 cabling systems already installed, making it a highly cost effective solution.

802.3u
The IEEE committee working on standards for Fast Ethernet.

ADSL
Short for asymmetric digital subscriber line, a technology that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).

ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

DHCP
An Ethernet protocol specifying how a centralized DHCP server can assign network configuration information to multiple DHCP clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.

DNS
Short for Domain Name System (or Service), an Internet service that translates domain names into IP addresses.
Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4. The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Domain Name
A descriptive name for an address or group of addresses on the Internet. Domain names are of the form of a registered entity name plus one of a number of predefined top level suffixes such as .com, .edu, .uk, etc. For example, in the address mail.NETGEAR.com, mail is a server name and NETGEAR.com is the domain.

DSL
Short for digital subscriber line, but is commonly used in reference to the asymmetric version of this technology (ADSL) that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).
ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

Dynamic Host Configuration Protocol
DHCP. An Ethernet protocol specifying how a centralized DHCP server can assign network configuration information to multiple DHCP clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.

Gateway
A local device, usually a router, that connects hosts on a local network to other networks.

IETF
Internet Engineering Task Force. Working groups of the IETF propose standard protocols and procedures for the Internet, which are published as RFCs (Request for Comment) at *www.ietf.org*.
An open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

IP

Internet Protocol is the main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.

IP Address

A four-byte number uniquely defining each host on the Internet, usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57).
Ranges of addresses are assigned by Internic, an organization formed for this purpose.

IPX

Short for Internetwork Packet Exchange, a networking protocol used by the Novell NetWare operating systems.
Like UDP/IP, IPX is a datagram protocol used for connectionless communications. Higher-level protocols, such as SPX and NCP, are used for additional error recovery services.

ISP

Internet service provider.

Internet Protocol

The main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.

LAN

A communications network serving users within a limited area, such as one floor of a building.

local area network

LAN. A communications network serving users within a limited area, such as one floor of a building.
A LAN typically connects multiple personal computers and shared network devices such as storage and printers. Although many technologies exist to implement a LAN, Ethernet is the most common for connecting personal computers.

MAC address

The Media Access Control address is a unique 48-bit hardware address assigned to every network interface card. Usually written in the form 01:23:45:67:89:ab.

Mbps

Megabits per second.

NetBIOS

The Network Basic Input Output System is an application programming interface (API) for sharing services and information on local-area networks (LANs).
Provides for communication between stations of a network where each station is given a name. These names are alphanumeric names, up to 16 characters in length.

Network Address Translation
NAT. A technique by which several hosts share a single IP address for access to the Internet.

NIC
Network Interface Card. An adapter in a computer which provides connectivity to a network.

packet
A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.

router
A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.

Routing Information Protocol
RIP. A protocol in which routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.

Subnet Mask
A mask used to determine what subnet an IP address belongs to. Subnetting enables a network administrator to further divide an IP address into two or more subnets.

TCP/IP
The main internetworking protocols used in the Internet. The Internet Protocol (IP) used in conjunction with the Transfer Control Protocol (TCP) form TCP/IP.

WAN
A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.

WEB Proxy Server
A Web proxy server is a specialized HTTP server that allows clients access to the Internet from behind a firewall.
The proxy server listens for requests from clients within the firewall and forwards these requests to remote Internet servers outside the firewall. The proxy server reads responses from the external servers and then sends them to internal client clients.

wide area network
WAN. A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.

Windows Internet Naming Service

WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.

If a remote network contains a WINS server, your Windows PCs can gather information from that WINS server about its local hosts. This allows your PCs to browse that remote network using the Windows Network Neighborhood feature.

WINS

WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.

Index

R

S

T

U

W